

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

April 2015





FOREWORD

April 10, 2015

We are pleased to present the 2015 Executive Order 13636 Privacy and Civil Liberties Assessments Report. On February 12, 2013, President Obama issued Executive Order 13636 (Executive Order), *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 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, the Executive Order requires federal agencies to develop and incentivize participation in a technology-neutral cybersecurity framework, to increase the volume, timeliness, and quality of cyber threat information it shares with the private sector, and to work with their senior agency officials for privacy and civil liberties to ensure that privacy and civil liberties protections are incorporated into all of these activities.

Section 5 of the Executive Order also requires that senior agency officials for privacy and civil liberties, in consultation with the United States Privacy and Civil Liberties Oversight Board ("the Board"), annually assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken pursuant to the Executive Order. The senior officials must submit those assessments to the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office for compilation and publication in this report. DHS released the first annual compiled report on April 10, 2014, which covered activities under the Executive Order that occurred during fiscal year 2013.

This second annual report provides assessments of activities under the Executive Order that occurred in fiscal year 2014. 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 Executive Order implementation. This year's report also incorporates constructive feedback and suggestions provided by the Board in response to the April 2014 report.

The chart below provides an overview of the departments and agencies that provided input for this year's report. We note that not all agencies were required to assess all sections of the Executive Order.

2015 Executive Order 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 Commerce (Commerce)	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	X	X		X
4(b) Dissemination of Cyber Threat Reports	X			X		X		
4(c) Enhanced Cybersecurity Services / Defense Industrial Base Program	X		X					
4(d) Private Sector Clearance Program		X						
4(e) The DHS Loaned Executive Program	X							
7(a) & 7(c) Voluntary Cybersecurity Framework					X	X		
8(d) Incentives for Voluntary Framework Participation					X			
9(a)/9(c) Critical Infrastructure Identification & Notification	X	X						
Other							X	

For comparison purposes, the chart below provides a summary of the departments and agencies that provided input for the 2014 report.

2014 Executive Order Section 5 Reports by Department and Topic

	DHS	Treasury	DoD	DOJ	Commerce	HHS	DOE	ODNI	GSA*	DOT*
4(a) Cybersecurity Information Sharing	X	X		X		X		X		X
4(b) Dissemination of Cyber Threat Reports		X		X				X		
4(c) Enhanced Cybersecurity Services / Defense Industrial Base Program	X		X							
4(d) Private Sector Clearance Program	X									
4(e) The DHS Loaned Executive Program	X									
7(a) & 7(c) Voluntary Cybersecurity Framework					X	X		X		X
8(a) Voluntary Critical Infrastructure Cybersecurity Program		X								X
8(d) Incentives for Voluntary Framework Participation		X			X	X				
9(a)/9(c) Critical Infrastructure Identification & Notification		X				X				X
Other									X	

*GSA = General Services Administration; DOT = Department of Transportation

Our offices – the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office – coordinated with the senior agency official(s) 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.

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

Our offices also facilitated communications among the senior agency officials and the Board. Each agency, however, worked independently and directly with the Board in its consultative role, 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 official(s)’ determination regarding which activities were required under the Executive Order, or were otherwise deemed appropriate, to be assessed. In future years, as the Executive Order is 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 under the Executive Order.



Megan H. Mack
Officer for Civil Rights and Civil Liberties



Karen L. Neuman
Chief Privacy Officer

TABLE OF CONTENTS

FOREWORD.....	2
PART I: DEPARTMENT OF HOMELAND SECURITY	7
PART II: DEPARTMENT OF THE TREASURY.....	50
PART III: DEPARTMENT OF DEFENSE	68
PART IV: DEPARTMENT OF JUSTICE.....	94
PART V: DEPARTMENT OF COMMERCE.....	122
PART VI: DEPARTMENT OF HEALTH AND HUMAN SERVICES	136
PART VII: DEPARTMENT OF ENERGY	143
PART VIII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.....	150

PART I: DEPARTMENT OF HOMELAND SECURITY



I. Introduction

Background and Scope

Section 5 of Executive Order 13636 (Executive Order) requires the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties to assess the privacy and civil liberties impacts of the activities the Department of Homeland Security (DHS, or Department) undertakes pursuant to the Executive Order and to provide 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 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 Order.

The first annual report, covering activities conducted by the Department during 2013, along with Privacy and Civil Liberties Assessments conducted by other departments was released as a combined document in April 2014.

This year's assessment covers Department activities conducted during fiscal year 2014. It includes a civil liberties assessment of new activities under Sections 9(a) and 9(c) of the Executive Order and also follows up on outstanding items and recommendations discussed in last year's assessment of activities under Sections 4(a), 4 (b), 4(c), and 4(e) of the Executive Order. As in last year's assessment, the scope of this year's assessment is limited to those DHS activities that were undertaken as a result of the Executive Order or substantially altered by it. Section 5 of the Order directs 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 which are driven by the Executive Order. More information on DHS's cybersecurity responsibilities and activities is available at: <http://www.dhs.gov/topic/cybersecurity>.

The DHS Privacy Office

The Privacy Office is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the Homeland Security Act (Homeland Security Act), as amended.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

The 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 Assessments

Section 5(b) of the Executive Order directs senior agency privacy and civil liberties officials of agencies engaged in activities under the order 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 this 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 Record 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 EO 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 fulfills the Department's mission to preserve, protect, and secure the homeland. The DHS Privacy Office applies the FIPPs to the full breadth and diversity of Department systems, programs, and initiatives that use personally identifiable information, 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), PIAs, and SORNs to ensure the implementation of the FIPPs at DHS.⁹ When conducting a Privacy Compliance Review (PCR)¹⁰, such as the one

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.

completed on 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 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 presented by any given program or activity vary greatly. This approach involves 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

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.

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

policies, operating procedures, other documentation or simple changes in program activities, as appropriate.

Related DHS Privacy and Civil Liberties Cyber Activities

Our work under the Executive Order is a continuation of the Department's efforts to provide transparency into its 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, the DHS Privacy Office and CRCL provide updates to the assessments they conducted last year under Executive Order Sections 4(a), (c), and (e), including explaining instances where implementation approaches have changed, and new civil liberties assessments of activities under Executive Order Sections 9(a) and 9(c). As the Department continues its implementation activities under the EO, 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(a): Cybersecurity Information Sharing:

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

Introduction

The Department undertook no new activities under Section 4(a) during this reporting period. As discussed in last year's assessment, the Department's June 2013 memorandum *Departmental Cyber Threat Information Sharing Procedures* (Shareline Memorandum), established the "Shareline" product line to implement Section 4(a). DHS interprets Section 4(a) as the unclassified release of a portion or excerpt of a dissemination-controlled cyber threat report

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>

(interpreted by the program offices as DHS-originated classified reports) to specific targeted entities, rather than general threat reporting to an entire sector (e.g., financial, energy, retail).¹⁴

In last year's assessment the Department also indicated that a Shareline directive and instruction would be forthcoming. Although the Department expected to identify DHS-originated classified cyber threat reports, it became evident that the vast majority of cyber threat reports originated in DHS are unclassified in the first instance in order to ensure a timely and wide distribution of releasable cyber threats to private critical infrastructure entities. The primary sources of information specific to a targeted entity are typically discovered by DHS law enforcement components in the course of an investigation and shared directly with the targeted entity—victim notification—through longstanding procedures that pre-date the Executive Order and fall outside the articulated Shareline process. Also, prior to the issuance of the Executive Order, two DHS non-law enforcement components, National Protection and Programs Directorate (NPPD) and the Office of Intelligence and Analysis (I&A), had already been sharing unclassified cyber threat reports (not DHS-originated classified products) with the private sector. Because cyber threat reports originating within the Department are primarily unclassified, a Shareline process designed to capture and appropriately disseminate DHS-originated classified information regarding cyber threats has not led to the production of any Sharelines or the issuing of a Shareline directive or instruction in Fiscal Year 2014 as originally contemplated. Accordingly, the Department is currently reevaluating the utility in using Sharelines to disseminate cyber threat reports and reconsidering its approach to best implement Section 4(a) of the Executive Order.

The Department noted in last year's report that Executive Order Sections 4(a) and 4(b) are closely related because any products created pursuant to Section 4(a) will be subject to the broader U.S. Government process for disseminating cyber threat information created under Section 4(b). As DHS works with other departments and agencies to conduct activities required under Section 4(b), we will be mindful of related activities that could fall within the scope of Section 4(a), and if such activities are occurring will assess them at that time.

¹⁴ The Department has a number of sharing programs to support this kind of general threat reporting that do not fall within the Department's specific interpretation of Section 4(a) and therefore are beyond the scope of this report.

Update on Fiscal Year 2013 Recommendations on Sharelines

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

Update: As discussed, the absence of a Shareline product line makes this recommendation obsolete.

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

Update: The absence of a Shareline product line makes this recommendation obsolete.

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

Update: The absence of a Shareline product line makes this recommendation obsolete.

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

Update: To the extent that Sharelines or other products are developed pursuant to section 4(a), the Privacy Office and CRCL will work to ensure that they incorporate privacy and civil liberties considerations at the outset.

Recommendation 5. *DHS should develop a tracking mechanism for Shareline dissemination, leveraging the processes developed under Executive Order Section 4(b). This will enhance the Accountability and Auditing Principle, which can reinforce implementation of the rest of the Fair Information Practice Principles.*

Update: The tracking mechanisms for disseminating DHS-originated unclassified cyber threat reports are still being developed through an interagency process. To the extent that DHS Component-originated disseminated reports may be developed, the Privacy Office and CRCL will follow the development of the tracking mechanism, and report as appropriate in a future Executive Order Assessment Report.

III. 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.

DHS participated in a pilot with the Federal Bureau of Investigation (FBI) to determine whether the Guardian system on the SECRET Internet Protocol Network Router (SIPRNET)¹⁵ could be leveraged to track the production and dissemination of cyber threat reports to targeted private sector critical infrastructure entities. As a result of this pilot and with guidance from the National Security Council (NSC) staff, FBI, DHS, and the Department of Defense (DOD) developed an interagency Joint Requirements Team (JRT) to develop requirements for a system that meets the Section 4(b) mandate. The Privacy Office and CRCL will monitor this progress and assess as appropriate in future Executive Order Assessment Reports.

IV. 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 ECS is a voluntary information sharing program that assists 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 providers¹⁶ and operational implementers¹⁷ (hereinafter "commercial service providers") that will enable them to better protect their critical infrastructure customers.

¹⁵ SIPRNET is a service gateway function that provides protected connectivity to federal, intelligence community, and allied information at the secret level.

¹⁶ The term Commercial Service Provider (CSP), refers to a public or private company is capable of providing managed security services for the protection of critical infrastructure customers. Any managed security service provider meeting the eligibility requirements may become a CSP.

¹⁷ The term Operational Implementer refers to a critical infrastructure organization that may choose to build their own infrastructure for the purposes of receiving, managing, and utilizing the DHS cyber threat indicators in the protection of their information assets, in effect to act as their own commercial service provider. The requirements for

The calendar year 2014 Privacy and Civil Liberties Assessment Report on Enhanced Cybersecurity Activities focused on discussing key foundational questions in the establishment and operation of the program. This year's assessment will provide a brief summary of the basic operation of that program, an overview of privacy, civil rights, and civil liberties oversight of the program, a description of the assessment methodology and, finally, the assessments of CRCL and the Privacy Office.

Basic Operation of the Program

Within the ECS program, the NPPD Office of Cybersecurity and Communications (CS&C) provides government furnished information, specifically indicators of malicious cyber activity¹⁸ to participating commercial service providers. An indicator is human-readable cyber data (e.g., related to Internet Protocol (IP) addresses, domains, email headers, files, and strings) used to identify some form of malicious cyber activity.¹⁹ These indicators can be used by the commercial service providers to create intrusion detection signatures,²⁰ or other means of detecting and mitigating cyber threats. A signature is a machine-readable software code that enables the automated detection of the known or suspected cyber threats associated with the indicators.²¹ DHS is not a party to the agreements between the commercial service providers and critical infrastructure owners and operators. The purpose of the program is to assist the owners and operators of critical infrastructure²² in enhancing their ability to protect their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program.

As a condition for receiving government-furnished information, commercial service providers agree to secure this sensitive information consistent with the Government's guidelines for the protection of national security information. If a critical infrastructure entity and its commercial service provider agree, then the commercial service provider may provide aggregated

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.

¹⁸ 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, without lawful authority. Information about cyber threats may be received from government, public, or private sources. Categories 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.

¹⁹ Indicators can be either unclassified or classified. Whether an indicator is classified is dictated by its source and whether the originator chooses to exercise original national security classification authority to control the dissemination of the indicator.

²⁰ Signatures are specific machine readable patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designed to delete files from a computer without authorization.

²¹ Additional information about indicators and signatures is addressed in the National Cybersecurity Protection System (NCPS) Privacy Impact Assessment, published July 30, 2012, and available at: <http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf>.

²² Critical infrastructure are the assets, systems, and networks, whether physical or virtual, that are so vital to the United States that their incapacitation or destruction would have a debilitating effect on physical and national economic security, public health or safety, or any combination thereof.

cybersecurity metrics information back to DHS.²³ Other than a DHS validation that an entity is a part of U.S. Critical Infrastructure, there is no relationship established under this program between DHS and that critical infrastructure entity.

Importantly, the ECS program does not involve the monitoring of communications by the Government, either directly or by proxy. Cybersecurity metrics provided to DHS about cyber threats encountered are aggregated, and do not include PII, monitored or collected content, or the identification of the critical infrastructure entity (unless otherwise agreed by the critical infrastructure entity or commercial service provider).

The roles of participants, and how they participate in this program, are described below.

Critical Infrastructure Entities: Section 4(c) of the Executive Order requires DHS to “establish procedures to expand the ECS program to all critical infrastructure sectors.” ECS is open to eligible critical infrastructure entities from all critical infrastructure sectors. Critical infrastructure entities seeking to participate in ECS program are required to contact one of the qualified commercial service providers, currently AT&T or CenturyLink, to begin the process to become a validated critical infrastructure entity. The commercial service providers in turn contact DHS for validation. DHS validates the critical infrastructure status by evaluating the entity to confirm it is an owner or operator of critical infrastructure systems or assets. DHS is not involved in the discussions between commercial service providers and potential critical infrastructure customers and is not otherwise involved in the relationship, unless the critical infrastructure owner or operator voluntarily chooses to have a broader engagement with DHS. More information about this onboarding process is available on the ECS program website at: <http://www.dhs.gov/enhanced-cybersecurity-services>.

Commercial Service Provider: Interested commercial service providers must enter into a memorandum of agreement with DHS and meet the security requirements set forth by the ECS program. Commercial service providers must agree to handle, use, and maintain all sensitive and classified information in accordance with Government-provided security requirements. An approved commercial service provider will be permitted to provide cybersecurity services to validated critical infrastructure entities. ECS can be offered to subscribing critical infrastructure customers as a stand-alone service, without requiring the commercial service provider to serve as the customer’s internet service provider. The relationship with the Government is strictly voluntary; the commercial service provider must provide enhanced cybersecurity services, but need not employ all cyber threat indicators it receives or all approved services or countermeasures (hereinafter “services” unless otherwise noted for clarity).²⁴

²³ The identities of operational implementers who encounter cyber threats cannot be redacted where those entities choose to report to DHS, since the operational implementers function as their own commercial service providers and their identity is therefore known to DHS.

²⁴ NIST 800-95 defines a service “as a processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems.” Countermeasures, which can be provided as services, are interpreted by the program to include automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system, for the purpose of protecting the information system from cybersecurity threats. As used in this report, the term “services” can be read to include countermeasures.

Operational Implementers: Operational implementers are validated critical infrastructure entities that are interested in receiving government-furnished information from the ECS to use in the protection of their own – and only their own – internal network. Operational implementers must enter into a memorandum of agreement with DHS that is identical in most respects to the agreements entered into by the commercial service providers with the exception that operational implementers do not provide services to other entities, and are not anonymous if they choose to provide information about cyber threats encountered. Operational implementers must meet the same security requirements as commercial service providers, and when the term “commercial service providers” is used in this document, it should be understood to include operational implementers, unless otherwise noted.

Government Furnished Information to Commercial Service Providers: The ECS program shares sensitive and classified government cyber threat information with qualified commercial service providers. In turn, commercial service providers use the cyber threat information to protect their customers who are validated critical infrastructure entities. The selection of cyber threat information that is provided to the commercial service providers occurs as a routine matter at the operational level within CS&C, acting in concert with government partners. Commercial service providers may provide aggregated and anonymized cyber metric information back to DHS in order to ascertain the effectiveness of cyber threat information sharing.

When using government-furnished information provided through this program, commercial service providers can only provide the types of services that are approved by DHS for use with this information. Restricting how this information is deployed on a commercial service provider’s network ensures the protection of government-furnished information from adversaries.²⁵

Commercial Service Provider’s Provision of Cybersecurity Metrics to DHS and DHS’s Use of those Metrics: Commercial service providers are permitted (not required) to provide metric information to the government for the purposes of assessing indicator and service effectiveness. This is voluntary and the commercial service provider or critical infrastructure entity can choose not to share any or all of its information with the government. The Memoranda of Agreement between DHS and the commercial service providers include a clause to this effect. The information shared with DHS is limited by that memorandum, and may include metrics information such as the following at the discretion of the critical infrastructure entity and the commercial service provider: the “fact of” a cyber threat detection; the indicator used; the number of hits per indicator per customer; the critical infrastructure sector in which the threat was detected, along with the date and time encountered; the source IP address; and the port and protocol that was targeted. Although the Memoranda of Agreement permits the sharing of the types of metrics described above, DHS standard operating procedures further limit the metrics the ECS Program routinely requests from commercial service providers. For more information on the metrics DHS routinely requests, please see subsection B, “Close Oversight and Advisory Involvement Serves as a Protective Measure,” of the “New Programmatic Protections of Individual Rights,” portion of the CRCL assessment. The metrics shared with DHS may prompt DHS to look at an indicator in greater depth, and this subsequent analysis may cause DHS to develop additional indicators.

²⁵ See *Executive Order 13636 Privacy and Civil Liberties Assessment Report*, April 2014, at pp 32-33. Available at <http://www.dhs.gov/publication/executive-order-13636-privacy-and-civil-liberties-assessment-report-2014>

DHS Sharing of Information Received Under Enhanced Cybersecurity Services: The ECS Program Management Office generates monthly reports utilizing the voluntary metric information DHS receives from commercial service providers, for the purpose of measuring program effectiveness. These monthly performance reports are shared with ECS partners consistent with the ECS Program Metrics and Reporting Standard Operating Procedures.

Privacy, Civil Rights, and Civil Liberties Participation

As noted in last year's assessment, CS&C is supported by CRCL, the NPPD Office of Privacy, the Office of the General Counsel (OGC), and the DHS Privacy Office, particularly in developing the 2013 ECS PIA. The collaboration among these offices continued in Fiscal Year 2014.

All four offices reviewed the implementing activities required under the Executive Order, and on a regular basis, the offices provided policy advice and oversight to NPPD elements, including the ECS Program Operations (National Cybersecurity and Communication Integrations Center (NCCIC)/ United States --Computer Emergency Readiness Team (US-CERT)) and the ECS Program Management Office. The NPPD Office of Privacy and CRCL also routinely provided advice and guidance to ensure that privacy and civil liberties were protected in the provision of government furnished information and in the approved services.

Assessment Scope and Methodology

CRCL: CRCL conducted reviews of program documentation, including policies, procedures, and reporting on the conduct of Enhanced Cybersecurity Services program activities. CRCL additionally conducted interviews with relevant program staff. Information incorporated into this Assessment was collected following the completion of Fiscal Year 2014, and also on a continuing basis during Fiscal Year 2014.

Privacy: The Privacy Office assessment includes (1) an updated, high-level analysis of the program's implementation of key aspects of the DHS FIPPs and (2) a summary of the results of its PCR on the ECS program, as noted in last year's assessment. Additional information on the PCR Process is included in the Privacy Assessment section.

CRCL Assessment

The focus of last year's assessment was to examine whether the government was using Enhanced Cybersecurity Services to unreasonably collect private sector or other non-Federal internet communications, either directly or by using the commercial service providers as a proxy to perform the collection. The assessment also addressed concerns that this program could be used to conduct targeted monitoring of individuals, either for criminal investigative or intelligence surveillance purposes.

In the Assessment Report on Enhanced Cybersecurity Services activities conducted during Fiscal Year 2013, CRCL found that the Government was not using the system to monitor or collect private sector and non-Federal Internet communications, that it was not susceptible to use for targeted monitoring of individuals and that the voluntary nature of participation was an important safeguard to protect against these concerns. The Enhanced Cybersecurity Services program has not substantially changed its manner of operations since that time, though it has begun to expand, and the program office has begun to expand its governance and operational policies accordingly.

This year's assessment of the civil liberties implications of the Enhanced Cybersecurity Services program is focused on how the program was implemented during Fiscal Year 2014, how civil liberties protections were incorporated into the policies governing the program, how CRCL advice was sought in deliberative decision-making, and how the program supported regular compliance review by sharing the metrics information returned to the Department by the commercial service providers. Following our review, CRCL determined that the policies, procedures and governance activities undertaken by the Enhanced Cybersecurity Services program have served to strengthen the program's posture with respect to the protection of civil liberties, and its participation with CRCL in developing policies and procedures to safeguard individual rights. CRCL concluded that, while there is still room for development as the program grows, the policies and procedures that serve to protect civil liberties are commensurate with the program's current stage of development.

New Programmatic Protections of Individual Rights

The Enhanced Cybersecurity Services program formalized policies and procedures that govern program operations, and took steps to ensure regular oversight office review, including, among other things, routine inclusion of CRCL in the making of significant governance decisions and routine compliance activities. Together, these measures directly or indirectly worked to protect individual rights. These measures include:

- a. **Policy and Standard Operating Procedures Developed to Protect Civil Liberties.** It is important for a program that routinely deals with complex activities and classified information to develop and institutionalize governance practices to appropriately address the possible civil liberties implications of proposed government actions. The Enhanced Cybersecurity Services program is in a relatively nascent stage, but has begun formalizing policies and processes to govern program activities, which collectively aid in the protection of privacy and civil liberties. These includes the following DHS guidance documents: 1) *Policy Principles*; 2) *Government Furnished Information Data Verification and Vetting Process*; and 3) *Service Expansion Workflow Process*, discussed below:

i. ***Policy Principles.*** All proposed services for use with DHS-provided cyber threat indicators must adhere to the principles articulated in the Enhanced Cybersecurity Services *Policy Principles* standards. All proposed services must adhere the following policy principles:

- Policy Principle #1 – Service deployment shall protect U.S. Government equities and provide appropriate operational security protections.
- Policy Principle #2 – Services should be implementable using commercial capabilities
- Policy Principle #3 – Services should increase security of protected networks.
- Policy Principle #4 – Appropriate government furnished information (GFI) should be available to support the new service.
- Policy Principle #5 – Services shall be limited to automated actions taken to modify, block or redirect data packets to protect a network, and shall not cause damage or provide unauthorized access to any other network or system.
- Policy Principle #6 – Services must adhere to the Fair Information Practice Principles to minimize the adverse impacts on privacy, and should apply appropriate protections of individual rights to ensure civil liberties are not violated.
- Policy Principle #7 - Services shall be deployed only for the purposes of defending against and preventing cybersecurity threats to protected information systems.

Policy principles 1 through 3 primarily address operational equities and how the Enhanced Cybersecurity Services program stays within appropriate operational boundaries and protects the integrity and security of the data it shares. Policy principles 4 through 7 address privacy and civil liberties concerns more directly by imposing limitations on DHS activity that may affect persons or networks. For instance, under Principle #5, approved services may only involve the analysis, modification, blocking, or redirection of data packets to protect a network; no other types of services are authorized, and the use of government-furnished information for services that might involve destruction of systems or unauthorized access is expressly prohibited. Principle #6 requires the protection of privacy via application of the Fair Information Practice Principles, and that any individual rights issues present be addressed with “appropriate protections to ensure civil liberties are not violated,” a protection that effectively requires the Program Office to seek guidance from the oversight offices. Finally, Principle #7 is a strict use limitation that prohibits the use of Enhanced Cybersecurity Services for anything other than cybersecurity and network defense purposes.

Articulation of a policy does not necessarily ensure protection of individual rights, but these principles are used to guide the methodical evaluation of the capabilities being proposed. The primary role of the *Principles* articulated in this policy is to establish baseline program guidelines, along with embedding the oversight offices within the deliberative process. This policy is primarily aimed at the evaluation of new services proposed by the Government, or by the commercial service providers, but it also drives other policies, including the policy discussed below governing the vetting of government furnished information.

Any proposed service undergoes review prior to being offered to commercial service providers. If a proposed service does not adhere to these guiding principles, then it fails the review and is not forwarded through the program for implementation by commercial services providers. The role of CRCL in this process is to review proposed services for civil liberties concerns and provide any relevant advice on potential ways to mitigate such risks where applicable.

- ii. ***Government Furnished Information Data Verification and Vetting.*** The systematic vetting of data to be furnished by the Government and utilized as government furnished information by commercial service providers is guided by DHS's *Government Furnished Information Data Verification and Vetting Process* (November 2013). The aim is to ensure that possible cyber threat information provided to the Enhanced Cybersecurity Services program is timely and appropriate in scope and type.

The procedures in the *Government Furnished Information Data Verification and Vetting Process* are consistent with the processes in place to minimize personally identifiable information and other sensitive information and vet cyber threat information, indicators and signatures within the National Cybersecurity Protection System.²⁶

As with threat information used in other capabilities operated under the ambit of the National Cybersecurity Protection System, the touchstone handling and use standard revolves around minimization of personally identifiable information or other potentially sensitive information (such as communications or proprietary content) in cybersecurity activities, unless that information is necessary for understanding or responding to the threat. The *Government Furnished Information Data Verification and Vetting Process* policy applies this standard in several ways within the Enhanced Cybersecurity Services program depending on the context in which the information is being handled. That policy directs that providers of government furnished information to the Enhanced Cybersecurity Services program (including DHS and other government sources) should not

²⁶ The National Cybersecurity Protection System is the Department's integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities that are used to defend federal civilian government networks from cyber threats, and for capabilities to share cyber threat information with critical infrastructure. Programs and activities within the National Cybersecurity Protection System program support the Enhanced Cybersecurity Services program, but are not assessed within this assessment because the National Cybersecurity Protection System program is not one of the activities directed by Executive Order 13636.

provide information that “contain[s] personally identifiable information unless it is necessary to understand or analyze the cyber threat. Indicators should be narrowly tailored to a cybersecurity threat and not capture extraneous information that could have an impact on Privacy and Civil Liberties.” This standard has been provided to other government agencies that provide cyber threat information to DHS to help them identify the types of information appropriate for sharing through the Enhanced Cybersecurity Services program.

DHS uses this same standard in vetting its cyber indicators, applying it with the assistance of oversight offices to cyber threat information developed by DHS and furnished to the commercial service providers. DHS analysts developing DHS cyber threat indicators are trained to follow standard operating procedures that address the identification, use, and handling of information that could be considered personally identifiable information. DHS does not include information that could be considered personally identifiable information in a cyber indicator shared through the Enhanced Cybersecurity Services program unless that indicator is necessary to detect or mitigate a cyber threat.²⁷ This standard is consistent with practices across all National Cybersecurity Protection System activities. DHS analysts are trained to identify and raise with oversight offices any information (whether shared cyber threat information, cyber threat indicators, or automated network screening templates or signatures) that could be considered personally identifiable information, or which are likely to implicate personally identifiable information when deployed.

The types of cyber threat data that may include personally identifiable information and which trigger this interaction typically include (but are not limited to) cyber threat indicators that may themselves contain personally identifiable information, or a proposed signature template or signature that contains, or is likely to capture, information that could be personally identifiable information when deployed.²⁸ For example, if DHS’s use of a particular network traffic screening signature is likely to capture personally identifiable information, then such a signature would be referred to oversight offices, including the NPPD Office of Privacy, the Office of the General Counsel, and CRCL, for review prior to deployment.

²⁷ For more information on this concept, see Sub-section 1, “Indicators – Identifying, Minimizing, and Marking Personally Identifiable Information as a Privacy Protection,” of the Privacy Assessment.

²⁸ Cyber threat indicators that are vetted under this process could be used in DHS-developed signatures, or shared under the Enhanced Cybersecurity Services program. All cyber threat information that could contain or implicate personally identifiable information, like all signatures that could contain or implicate personally identifiable information, is evaluated under the same standard. Signatures are based on and derivative of cyber threat indicators, and signatures developed by DHS are only for use in DHS cybersecurity programs such as the National Cybersecurity Protection System’s EINSTEIN capabilities, a DHS activity to secure U.S. Government networks which is not within the scope of this Executive Order. Cyber threat indicators (but not signatures) may also be shared with commercial service providers when they meet the standards articulated in the Policy Principles, and the Government Furnished Information Data Verification and Vetting Process. When a commercial service provider decides to use a particular indicator shared under Enhanced Cybersecurity Services, the provider develops and deploys a signature which is tailored to operate effectively on their own unique network architecture.

This referral starts a review process between the program and the oversight offices, to determine whether using such an indicator is necessary for characterizing or mitigating the identified threat, or if some narrower sharing of technical information, without personally identifiable information, would be sufficient. The intent is to minimize the sharing of personally identifiable information or other sensitive information linked to individuals in indicators, and to minimize the possible effect on personally identifiable information or individuals' communications once the indicators are crafted into a signature. The policy for government furnished information provided to DHS also contains other standards for timeliness and reliability of the information deployed, to ensure that commercial service providers are given up-to-date information that is responsive to actual threats, rather than outdated information that could lead to the impairment of network traffic that is not malware. The policy also describes the types of cyber threat information that should be considered for sharing, including among other things malware, exploits, filenames, Uniform Resource Locators, Internet Protocol addresses, and other types of data that are sometimes associated with particular cyber threats. The aim is to solicit from other Government agencies and sources within DHS only that cyber threat information that might be helpful in mitigating the threat against the critical infrastructure sectors, while also consistently minimizing the collection, use, retention and sharing of personally identifiable information and other sensitive types of information. Although this assessment is focused on those instances where personally identifiable information and other sensitive information, such as communicative content must be shared to characterize a threat, the bulk of the information sharing involves various types of technical information, as reflected in this list.

- iii. ***Service Expansion Process Flow.*** During Fiscal Year 2014, DHS instituted the addition of the *Service Expansion Process Flow* (December 2013). This process is triggered when the Government determines that a proposed service – service – fitting within the broad guidelines of the Enhanced Cybersecurity Services *Policy Principles* could improve the cybersecurity posture of protected entities. It is also triggered when a commercial service provider suggests offering a new or additional service based upon the Government Furnished Information. This process spells out a formal DHS and interagency vetting process to ensure that such changes in the program are subjected to thoughtful, comprehensive deliberation using the vetting process to work through the relevant operational and oversight implications, as well as any interagency equities.

Under the *Service Expansion Process Flow*, when a new service is proposed, the Enhanced Cybersecurity Services program confers with the commercial service providers to discuss the feasibility and desirability of the proposed service, and to flesh out the details about how it *might* be implemented. A *Policy Principles* review then ensues at DHS to consider whether the proposal is consistent with the rules of the road prescribed for the program; the Enhanced Cybersecurity Services program office staff, operational personnel within CS&C, and the oversight

offices participate. This review might also result in appropriate modifications to ensure that the service will meet applicable operational and oversight office requirements. If approved by CRCL and the other staff and oversight offices, the proposal then undergoes legal review. If legally approved, the proposal then precedes either to interagency review within the National Security Staff-led Interagency Policy Committee for Cybersecurity or, if the proposal does not implicate interagency equities, then it is presented for approval to the DHS Secretary. Although new, this process was used effectively twice during Fiscal Year 2014. One proposed new service was approved, while another proposed service was withdrawn following the deliberative discussion.

b. Close Oversight and Advisory Involvement Serves as a Protective Measure.

The Enhanced Cybersecurity Services program worked in Fiscal Year 2014 to establish a good working relationship with CRCL.²⁹ A key governance feature of the Enhanced Cybersecurity Services program is embedding NPPD Office of Privacy and OGC staff within CS&C, in addition to adding regular consultation with CRCL. Both the Enhanced Cybersecurity Services program office and CS&C operational staff participate in these activities. These offices are engaged by CS&C staff and the Enhanced Cybersecurity Services program on a myriad of issues that are not all directly relevant to this Assessment. This close advisory relationship serves a dual purpose of helping the program stay focused on its mission, while allowing the oversight offices to work together with the programs to create operational and compliance policies that respond to privacy, civil liberties and legal concerns when appropriate.

A close working relationship is important because the technical nature of the cybersecurity problem set changes frequently, requiring fresh operational and policy approaches. Even though many of the same advisory and oversight challenges arise frequently, there are significant variations that merit detailed assessment by policy advisors on each occasion.

As discussed above, CRCL participates directly in advising CS&C when DHS-developed cyber threat information³⁰ or signatures could contain or implicate personally identifiable information, consistent with the policies and procedures governing the National Cybersecurity Protection System. The United States Computer Emergency Readiness Team (US-CERT) handles and develops cyber threat information that is used to support Enhanced Cybersecurity Services and National Cybersecurity Protection System activities. When cyber threat information or signatures that could be considered

²⁹ In last year's Privacy and Civil Liberties Assessment of the Enhanced Cybersecurity Services program, CRCL concluded about that "[o]ngoing vigilance is necessary due to the ever-present threat of mission-creep, and because as programs evolve and grow, new and frequently unanticipated civil liberties concerns may arise." *Executive Order 13636 Privacy and Civil Liberties Assessment Report*, April 2014, at 33.

³⁰ When DHS receives information from other government entities for use in ECS, DHS relies on those entities to comply with the policy principles described above. This is accomplished via the terms of the memoranda of agreement with those entities, and via sharing of the *Government Furnished Information Data Verification and Vetting Process* policy, which provides detailed guidance on what information is suitable for sharing with Commercial Service Providers through the Enhanced Cybersecurity Services program, as well as instructions for minimization.

personally identifiable information³¹ or are likely to implicate personally identifiable information are developed, the US-CERT analyst handling the matter is required by US-CERT policy to provide notice to US-CERT leadership and reach out to OGC, NPPD Office of Privacy, and CRCL to trigger a closer review. As noted above, this is a standard procedure within US-CERT, which is followed regardless of which activity is being supported, and the *Government Furnished Information Data Verification and Vetting Process* policy is just a version of that procedure which is specific to Enhanced Cybersecurity Services.

Following notification, US-CERT and the programs involved in sharing or using the information then work with the oversight offices to seek less intrusive means to effectively characterize the threat and enable appropriate response by commercial service providers, with the goal of finding a way to characterize the threat and permit mitigation without using that information. That inquiry frequently requires deliberation across several programs, as it may include discussion of other technical and operational options, such as sharing different elements of threat information, or sharing different pieces of information associated with the threat, which might help commercial service providers detect and deter threats in a less intrusive way. This narrower sharing might be accomplished by not including personally identifiable information and/or context information about the threat, while still providing enough cyber threat information to be actionable. Identifying the personally identifiable information that is necessary to characterize and respond to a threat is context dependent. The amount of information that must be shared and the degree of necessity present varies depending on the technical nature of the cyber threat, its severity, and the nature and quantity of information about the threat available to DHS. It may be easier to find alternative means to characterize and mitigate a threat when there is a large amount of information available regarding that threat, or where there are multiple plausible methods of mitigation available.

This process is regularly initiated by US-CERT as needed, which was approximately once monthly during Fiscal Year 2014. CRCL does not separately track which information might be shared under the Enhanced Cybersecurity Services program, because the minimization standard applied by CRCL is the same regardless of the program or activity supported.

c. **Routine Operational and Oversight Reporting.** In an effort to track program performance, the Enhanced Cybersecurity Services program provides monthly reports of its operational activities to appropriate DHS Stakeholders, including CRCL, OGC, and

³¹ CS&C uses the phrase “information that could be considered personally identifiable information” 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 an Internet Protocol address and domain information. In the context of ECS, 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. Given the nature of cyber threats and internet anonymity generally, it may also be difficult to confirm whether a particular piece of information is actually personally identifiable information – e.g., a true name of a real person – or just a convenient fiction, a spoofed name used by an adversary in the communication in question. In such cases, anonymity possesses considerable limitation to identifying and notifying those potential anonymous victims, and or performing redress.

the NPPD Office of Privacy. This reporting established programmatic accountability to responsible leadership, and facilitated programmatic oversight.

These reports include the types of government furnished information (“*Government Furnished Information Report*”) shared with commercial service providers. The metrics the commercial service providers may provide to DHS³² are defined by written policy limiting the types of data the Enhanced Cybersecurity Services Program may receive. The commercial service providers have been apprised in writing regarding those data elements, and have been informed that they may choose to provide any or none of that data. The data that may be provided to the program by the commercial service providers includes the following:

- **Sector:** Critical Infrastructure Sector associated with the indicator activity
- **Reference ID:** Indicator Identification
- **Date:** Date of the indicator activity
- **Time:** Time of indicator activity
- **Hits:** # of times the activity occurred
- **Service** – Countermeasure/Service

The metric data received from the commercial service providers is contained in the *ECS Monthly Program Performance Report*, and shared with CRCL and the other oversight offices each month. The program also produces a monthly classified report containing the same data, but adding additional threat information relating to the indicators that were active and, where appropriate, the threat actors involved. This provides more detail regarding the classified information sharing activities within the program, and the role that classified information sharing play in helping defend protected critical infrastructure from identifiable threat actors. Routine sharing of these reports with CRCL and the other oversight offices began in March 2014, immediately after the program office began assembling them on a regular basis. In addition to the monthly reporting of operational activities conducted within Enhanced Cybersecurity Services, the program also provided periodic updates on the status of new commercial service providers ‘entry into the program, as well as updates on programmatic or policy initiatives.

Civil Liberties Risks and Impacts

As noted above, there has been no substantial programmatic change in the operation of the Enhanced Cybersecurity Services program since the 2014 Assessment, other than the addition of new participants, and the development of additional policy to manage and govern the program

As we found in last year’s assessment, the risks of the Enhanced Cybersecurity Services program to civil liberties remain modest, as long as the Enhanced Cybersecurity Services program stays within the established parameters of the program including: 1) voluntary participation by

³² Because participation in the Enhanced Cybersecurity Services program is voluntary, commercial service providers are not required to provide feedback to the Department, but only to appropriately secure any government furnished information and to provide enhanced cybersecurity services to critical infrastructure. If they choose to provide feedback to DHS, the program office asks that the feedback be limited to the types of information described above.

commercial service providers and critical infrastructure entities; 2) no Government monitoring or access to private communications, including content; and 3) no Government receipt of the results of monitoring, other than metrics relating to the cyber threats encountered by the commercial service providers.

Although the policies and procedures discussed herein still reflect the program's relative youth, they provide appropriately detailed procedural tools to help Enhanced Cybersecurity Services program and CS&C operational staff operate the program within appropriate boundaries protective of individual rights. Specifically, the *Policy Principles, Government Furnished Information Data Verification and Vetting Process* and the *Service Expansion Workflow Process* work to provide rules of the road governing program operation, with individual rights protections embedded in those policies. Moreover, they require the systematic vetting of major program decisions by the oversight offices, and even though governing the activities of the commercial service providers is beyond the scope of the DHS role in this program, the policies governing the program's receipt of information limits the materials received by the program office to the metrics data described above.

The ongoing collaboration of DHS's advisory and oversight offices also helps to ensure the program maintains appropriate protections of individual rights as it grows and evolves. In our routine oversight and advisory involvement with the program during Fiscal Year 2014, CRCL found no irregularities and no instances of non-compliance with the policies described above, and the annual review conducted for this assessment of those materials (including all classified and unclassified metrics shared with DHS) and program policies, along with and additional fact-finding discussions with program staff, confirmed the program is in compliance with applicable policy guidelines. The voluntary nature of Enhanced Cybersecurity Services participation by commercial service providers and critical infrastructure entities – which is a key civil liberties protection – makes it impossible to require those participants to adopt specific privacy or civil liberties protective policies. Nevertheless, a review of all unclassified and classified metrics information produced from the program provided assurance to CRCL that the cybersecurity providers themselves – who are beyond the oversight reach of this office – were participating in the Enhanced Cybersecurity Services program in a way that complied with the written policies discussed above. Of particular relevance to civil liberties, the ECS program does not receive the content of communications from the commercial service providers.

As a result of the program office's inclusion of CRCL in all relevant program and policy activities, and CRCL's resulting visibility into the relationship with the commercial service providers, CRCL concludes that the risks to civil liberties, characterized as "modest" in last year's Assessment report, have been further addressed and mitigated. Consistent with our findings in last year's assessment, CRCL notes that ongoing vigilance is necessary due to the ever present threat of mission creep, and because as programs evolve and grow, new and unanticipated civil liberties concerns may arise. The Department and the ECS Program have addressed civil liberties concerns appropriately at this stage in the program's development, but must continue to build policies that preserve the voluntary nature of program participation, and which protect individual rights as the program is implemented and continues its growth.

Privacy Assessment

High-Level FIPPs Analysis

Transparency: The ECS program exhibits a high level of transparency, providing information to the public through a variety of mechanisms and fora. NPPD’s robust transparency efforts include: the publication of information and fact sheets on its public-facing website;³³ congressional testimony;³⁴ participation in public conferences and meetings; briefings to privacy, civil rights, and civil liberties advocates; public briefings to the DHS DPIAC;³⁵ the publication of a PIA;³⁶ and the publication of a public-facing PCR report.³⁷ Commercial service providers also publish information on the ECS program as part of their efforts to provide services to qualified critical infrastructure entities.

Data Minimization: Data minimization is at the core of DHS’s implementation of the ECS program. It is important to stress that DHS only shares information that could be considered PII under the ECS program if the information is necessary to detect or mitigate a cyber threat. This concept is described in depth in Subsection 1 below, “Indicators – Identifying, Minimizing, and Marking Personally Identifiable Information as a Privacy Protection.”

Individual Participation: Opportunities for individual participation in this context are very limited, as the relationship between DHS is with commercial service providers and not with members of the public. Broadly speaking, there are two categories of individuals who could be potential victims of cyber threats who may be impacted by the lack of individual participation—authorized users of critical infrastructure entities’ networks and members of the public interacting with critical infrastructure entities.

It is not feasible for the Government to provide redress for individuals PII may be included in a cyber threat indicator because they are the victim of a cyber threat. In part, the difficulty lies in determining whether a particular piece of cyber threat information is actually PII, such as the name of a real person, or a convenient fiction designed to facilitate the cyber threat, such as a fictional name created to mask the identity of the perpetrator of the cyber threat.

As further discussed in Subsection 4 below, “Notice as a Privacy Protection,” all authorized users of a participating critical infrastructure company’s network are to be under written notice that information and data on the network may be monitored or disclosed to third parties, and/or that the network users’ communications on the network are not private. For example, employees of a critical infrastructure company may see an electronic login or banner informing them that their activities on the network may be monitored or disclosed to third parties. Employees of a critical infrastructure company are then free to adjust their behavior accordingly.

³³ See <http://www.dhs.gov/enhanced-cybersecurity-services>.

³⁴ See multiple written testimonies available at: http://www.dhs.gov/news-releases?field_taxonomy_topics_tid=170.

³⁵ See <http://www.dhs.gov/dhs-data-privacy-and-integrity-advisory-committee-meeting-information>.

³⁶ See DHS/NPPD/PIA-028 Enhanced Cybersecurity Services, January 16, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

³⁷ See “Privacy Compliance Review of the Enhanced Cyber Security Services (ECS) Program,” available at: www.dhs.gov/privacy.

As noted in the FIPPs analysis of “Data Minimization” and described in depth in Subsection 1 below, “Indicators – Identifying, Minimizing, and Marking Personally Identifiable Information as a Privacy Protection,” DHS implements data minimization to limit the instances where information that could be considered PII is shared to only those cases where sharing the information is necessary to detect or mitigate the cyber threat. This data minimization helps to reduce the impact of limited individual participation by limiting the situations in which an individual may be impacted.

Purpose Specification: Purpose specification requires DHS to articulate the need to collect a particular piece of information. This justification informs DHS’s establishing a retention period for the information based on the mission need, and the FIPP of Data Minimization requires DHS to limit its collection and retention of information to that which is necessary to support the purpose for which the information is collected. DHS has proposed a retention schedule to the National Archives and Record Administration (NARA) that would cover all cyber threat information under the National Cybersecurity Protection System. This retention schedule would cover DHS’s retention of indicators shared under the ECS program.

DHS collects the cyber threat information for cybersecurity purposes, such as detecting or blocking a cyber threat. Under the proposed retention schedule, 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. This retention schedule is meant to reflect the fact that cyber threats may reactivate at a later date. For example, if DHS uses an indicator to develop a signature to detect or block a cyber threat, DHS would not want to remove the signature or delete the threat information until the threat is completely mitigated, in case the threat reappears at a later date. Deleting the information too early would re-open the vulnerability to the cyber threat.

Under the proposed retention schedule, 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). This retention period reflects purpose specification in that DHS is collecting information for cybersecurity purposes and is therefore not interested in information that is determined not to be related to known or suspected cyber threats or vulnerabilities.

Use Limitation: DHS collects cyber threat information for cybersecurity purposes. To ensure the use of the information is consistent with the cybersecurity purpose for which it was collected, indicators shared under the ECS program are provided to commercial service providers for the sole purpose of providing approved Enhanced Cybersecurity Services to critical infrastructure entities. Commercial service providers are not allowed to use the information for other purposes, even purposes that seem compatible, such as providing cybersecurity services to non-critical infrastructure entities.

As described in Subsection 6, “DHS’s Application of Privacy Protections to its Sharing of Cybersecurity Metrics and Indicators Developed as a Result of the Subsequent Analysis of Cybersecurity Metrics,” DHS may receive cybersecurity metrics from commercial service providers consistent with their commercial contracts with critical infrastructure entities. DHS may only share these cybersecurity metrics with other U.S. Government entities with cybersecurity responsibilities.

These use limitations are memorialized in the agreement between DHS and the commercial service providers.

Data Quality and Integrity: DHS performs both initial vetting and periodic reviews of indicators shared through the ECS program to promote data quality in the cybersecurity indicators. DHS has a mission imperative to promote data quality, as inaccurate indicators will not effectively detect or mitigate cyber threats or may block legitimate traffic. In accordance with standard operating procedures, DHS provides data quality criteria to Federal partners that share indicators with DHS, so that partners are aware of the data quality standards of the ECS program.

Security: As noted in Subsection 3, “Access and Security Controls as a Privacy Protection,” DHS employs robust access and security controls to ensure that only authorized users with a need-to-know are able to access the indicators shared under the ECS program.

Accountability and Auditing: DHS has implemented accountability and auditing in the ECS program through the Quarterly Privacy Reviews identified in Subsection 8, “Oversight and Accountability as a Privacy Protection,” and through the PCR summarized in this assessment. Both of those accountability mechanisms are designed to address the effectiveness of the existing privacy policies in practice.

Summary of the Privacy Compliance Review

The DHS Privacy Office conducted a PCR of the ECS Program,³⁸ in coordination with NPPD/CS&C and the NPPD Office of Privacy. Key findings from the PCR are summarized below. While the PCR addresses the effectiveness of the program’s existing privacy protections, this summary is designed to provide a high-level overview of key results. The PCR report may be accessed at www.dhs.gov/privacy for more detailed information on the results of the review.

The baseline of a DHS PCR is a program’s existing privacy compliance documentation. DHS also uses its FIPPs to evaluate any issues that may arise outside of the privacy compliance documentation. For ECS, the baseline of the PCR was its 2013 PIA.³⁹

ECS is an information sharing program that shares cybersecurity indicators that are received through other DHS programs or processes. To conduct a full PCR of ECS, the DHS Privacy Office also reviewed cybersecurity indicator development and processing that occurs through other DHS programs or processes, if those programs or processes are referenced or described in the ECS PIA. To assess ECS’ overall compliance with the existing PIA, the DHS Privacy Office developed and administered a questionnaire to NPPD that included an array of questions based on the ECS PIA; conducted follow-up engagement with NPPD on its responses to the questionnaire; and reviewed a variety of documentation specific to ECS or related to activities that occur outside of ECS, but are necessary for its operation and are referenced or described in the ECS PIA.

³⁸ See “Privacy Compliance Review of the Enhanced Cyber Security Services (ECS) Program,” available at www.dhs.gov/privacy.

³⁹ See DHS/NPPD/PIA-028 Enhanced Cybersecurity Services, January 16, 2013, available at: http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

The ECS PCR report followed DHS’s standard four-step process for PCR reports, which includes: 1) a description of the requirements from the ECS PIA, which are derived from the DHS FIPPs; 2) the DHS Privacy Office’s review of the requirements; 3) the DHS Privacy Office’s findings of compliance or non-compliance based on the review of the requirements; and 4) the DHS Privacy Office’s recommendations, if applicable. The first step in this process—a description of the requirements from the ECS PIA—serves as the metrics against which the DHS Privacy Office evaluates the program. A full description of the metrics and the DHS Privacy Office’s findings are available in the PCR report.⁴⁰

1. Indicators – Identifying, Minimizing, and Marking Personally Identifiable Information as a Privacy Protection

DHS may share DHS-developed indicators that may contain information that could be considered PII as part of ECS, but that information will only be shared under ECS if it is determined to be an indicator of a known or suspected cyber threat. NPPD has appropriate procedures to identify, minimize, and mark indicators that contain information that could be considered PII. Analysts follow standard operating procedures to identify, review, and, as appropriate, redact information that could be considered PII. If PII is identified, analysts are required to review and redact PII unless it is necessary for US-CERT analysts to protect an information system from cybersecurity threats, mitigate against such threats, or respond to a cybersecurity incident. Because different sets of terms may be used to explain when DHS collects, uses, or shares information that could be considered PII in its cybersecurity programs, it is important to clarify that information that could be considered PII will only be shared under ECS if it is part of the actual cyber threat and is therefore included in an indicator of a cyber threat. For example, the ECS PIA uses two sets of terms—“analytically relevant” or “directly relevant” (also “directly related”)—to describe the standards for handling information that could be considered PII. Although these sets of terms are sometimes used interchangeably, information that is “directly related” to a cybersecurity threat would be an indicator that could be used to actually detect or block the cybersecurity threat. Information that is “analytically relevant” could be information that could be used to detect or block a cybersecurity threat, but it could also be information that is important to understand the nature of the threat. US-CERT may retain either type of information under its Cybersecurity Information Handling Guidelines. However, only information that is “directly relevant” or “directly related” will be shared under ECS.

When information that could be considered PII is included in an indicator, it is because it is information that is “directly related” or “directly relevant” to a cybersecurity threat and is therefore necessary to protect against or mitigate such threats. Because DHS only shares indicators of cybersecurity threats under ECS, only information that is “directly relevant” or “directly related” is shared with commercial service providers under ECS as part of the known or suspected cybersecurity threat.

An example of information that could be considered PII that is “directly related” or “directly relevant” to a cybersecurity threat is a legitimate email address that may be

⁴⁰ See “Privacy Compliance Review of the Enhanced Cyber Security Services (ECS) Program,” available at: www.dhs.gov/privacy.

spoofed from a legitimate website that has been compromised. A cyber threat actor may use the compromised email address to launch a spear phishing campaign. Because the email address is the actual threat vector, there are no ways to prevent this type of attack without developing a signature to detect emails or attachments from that specific email address.

For indicators DHS receives from government cybersecurity partners, the *Government Furnished Information Data Verification and Vetting Process* policy requests that providers of government furnished information should not provide information that “contain[s] personally identifiable information unless it is necessary to understand or analyze the cyber threat. Indicators should be narrowly tailored to a cybersecurity threat and not capture extraneous information that could have an impact on Privacy and Civil Liberties.” This standard has been provided to other government agencies that provide cyber threat information to DHS to help them identify the types of information appropriate for sharing through the ECS program.

2. Preventing DHS from Accessing Personally Identifiable Information or the Contents of Commercial Service Providers’ Communications as a Privacy Protection

ECS consists of sharing indicators with commercial service providers by offering two cybersecurity services—Domain Name System (DNS) Sinkholing and Email Filtering. These services are approved by DHS but are implemented by the commercial service providers. DNS Sinkholing allows commercial service providers to redirect traffic from malicious domains to “safe servers” or “sinkhole servers” to prevent further malicious activity. The Email Filtering capability allows commercial service providers to scan, and potentially quarantine, email destined for critical infrastructure companies’ networks, in order to detect malicious content before the email is delivered to company end-users.

A key privacy concern is whether DHS would be accessing PII or the contents of commercial service providers’ communications through these services. DHS does not collect PII or access the contents of commercial service providers’ communications through these services. For the specific capabilities provided, the commercial service providers may supply hardware and develop software for ECS. DHS provides the cybersecurity indicators, as well as security requirements to ensure that the capabilities appropriately protect government-provided information from unauthorized disclosure through the service. DHS cannot and does not access content or metadata associated with any messages through the Email Filtering capability. The fact that DHS does not collect PII from or access the contents of commercial service providers’ communications under ECS is an important privacy protection based on the DHS FIPPs of Purpose Specification and Use Limitation that allows DHS to provide information to commercial service providers without collecting unnecessary information.

3. Access and Security Controls as a Privacy Protection

At DHS, ECS information is stored in the National Cybersecurity Protection System (NCPS) Mission Operating Environment (MOE), which exists on both unclassified and classified networks. We found that NPPD has robust security requirements for the NCPS

MOE. The NCPS MOE is separate from the DHS enterprise, meets Federal Information Processing Standard (FIPS) 199 standards, and applies National Institute for Standards and Technology (NIST) Publication 800-53 controls. NPPD has implemented processes to ensure that only authorized users with a need-to-know are allowed to access these operating environments, and NPPD has also implemented safeguards to ensure need-to-know is validated and user accounts are regularly reviewed to ensure accounts are maintained or deactivated as appropriate. NPPD also regularly reviews audit logs for both the unclassified and the classified MOE. Implementing these safeguards is an important security control.

Commercial service providers are also required to abide by robust security requirements to protect ECS information from unauthorized disclosure. DHS shares both classified and unclassified indicators with commercial service providers through secure channels. Commercial service providers receive, store, and use indicators in secure, classified facilities. The use of these secure, classified channels and facilities provides an additional layer of security to prevent the unauthorized disclosure of cybersecurity indicators.

NPPD has received no reports of unauthorized disclosures of indicators through the ECS Program. In the event of an unauthorized disclosure, NPPD would follow DHS and US-CERT-specific standard operating procedures for incident handling.

4. Notice as a Privacy Protection

Notice is one of the DHS FIPPs, and NPPD has worked diligently to implement mechanisms in ECS to ensure end users are receiving adequate notice. Consequently, one privacy protection embedded in ECS is that all authorized users of the participating critical infrastructure companies' networks will be under written notice, either through an electronic banner or otherwise, that information and data on the network may be monitored or disclosed to third parties, and/or that the network users' communications on the network are not private.

Because this is a voluntary program and DHS does not have a relationship with the participating critical infrastructure companies beyond certifying their eligibility, DHS uses the Memorandum of Agreement with commercial service providers to provide the notice requirement. The Memorandum of Agreement requires commercial service providers, prior to providing ECS to any protected entity, to "obtain a representation from such protected entity that, during the duration of such protected entity's participation in ECS, all authorized users of the protected entity's network will be under written notice, through an electronic login banner or otherwise, that information and data on the network may be monitored or disclosed to third parties, and/or that the network users' communications on the network are not private." The commercial service providers maintain private contractual agreements with their clients, and DHS is not party to those agreements. In keeping with the voluntary nature of commercial service providers' participation in the program, DHS does not monitor the commercial service providers' client-side implementation of ECS to ensure compliance with the terms and conditions of the memorandum of agreement.

5. Privacy-by-Design in Commercial Service Provider Feedback to DHS as a Privacy Protection

NPPD implements three important privacy-by-design controls to limit the possibility that information that could be considered PII may be inadvertently provided to DHS by commercial service providers.

First, DHS's Memoranda of Agreement with commercial service providers limit the information they may provide to DHS. Commercial service providers may, with the permission of the participating critical infrastructure client, provide limited and aggregated cybersecurity metrics to DHS. Permissible metrics include those such as: the number of hits (and source IP addresses), per indicator per customer (name redacted, unless otherwise agreed by customers), per given time period; whether a link or attachment was included in the e-mail and if an attachment was included, the attachment type; and metrics specific to DNS redirection.

Second, DHS requests that commercial service providers send metrics information to DHS in a standardized spreadsheet format. This standardized format does not include any fields that request PII.

Third, as DHS approves services for ECS, it considers whether technical controls may be implemented to prevent information that could be considered PII from being shared with DHS.

6. DHS's Application of Privacy Protections to its Sharing of Cybersecurity Metrics and Indicators Developed as a Result of the Subsequent Analysis of Cybersecurity Metrics

DHS may only share the cybersecurity metrics it receives from commercial service providers with U.S. Government entities with cybersecurity responsibilities. Information sharing agreements and standard operating procedures govern DHS's sharing cybersecurity information with other entities. For example, DHS has Memoranda of Agreement with Federal agencies participating in EINSTEIN, or US-CERT may share information with law enforcement and intelligence partners through liaisons detailed to US-CERT, consistent with standard operating procedures.

The metrics DHS receives from commercial service providers may prompt DHS to look at an indicator in greater depth, and this subsequent analysis may cause DHS to develop additional indicators. Any indicators that DHS may develop through this subsequent analysis would be developed according to US-CERT processes for all cybersecurity indicators. Similarly, those indicators would be shared according to agreements (e.g., EINSTEIN) or standard operating procedures. Consequently, it is important to note that any indicators developed through this subsequent analysis would have the same privacy protections included in all indicator development and would be shared according to DHS's information sharing agreements and standard operating procedures. This potential for subsequent analysis allows the ECS program to strengthen the cyber ecosphere in a privacy-protective manner.

7. Training as a Privacy Protection

All DHS employees and contractors receive standardized privacy awareness training. Additionally, NPPD began implementing cybersecurity-specific privacy training in June 2014 to provide in-depth, context-specific training for its analysts. The cybersecurity-specific training provides an overview of basic privacy concepts; identifies key triggers of privacy requirements in US-CERT's work; provides an in-depth review of requirements related to US-CERT's collection, processing, safeguarding, retention, and dissemination of information; outlines various accountability mechanisms for US-CERT's handling of personally identifiable information; and provides a list of resources (e.g., points of contact, specific standard operating procedures) for analysts to use later.

8. Oversight and Accountability as a Privacy Protection

The CS&C Oversight and Compliance Officer and NPPD Senior Privacy Analysts conduct quarterly internal reviews to evaluate and assess compliance with information handling procedures. While these reviews are not specific to ECS or how information is used in ECS, these Quarterly Privacy Reviews provide an opportunity for DHS oversight officials to conduct a timely and in-depth analysis of CS&C/US-CERT's information handling procedures. The reviews cover an impressive array of topics, including but not limited to standard operating procedures and checklists; reviews of signatures and signature templates; information sharing activities; and retention. The Privacy Office finds that these reviews have been very effective and enable NPPD to identify privacy risks and mitigations as the program evolves and matures.

Recommendations

Civil Liberties: CRCL determined in this assessment that the Enhanced Cybersecurity Services program has developed civil liberties protections commensurate with its current stage of development and demonstrated compliance with applicable laws, policies and procedures to protect individual rights. As the program matures and grows, it is incumbent on both the program and the Office for Civil Rights and Civil Liberties to continue the close advisory and oversight relationship established up to this point, and to work diligently to ensure that appropriate protections of individual rights continue to be built into the program's governance policies, and to monitor compliance with those policies by reviewing the information provided from the cybersecurity providers to the Department under this program.

Privacy: The sensitivities surrounding cybersecurity programs generally and the cooperation between the public and private sectors require robust privacy oversight. NPPD has demonstrated exemplary attention to implementing strong privacy protections in ECS and its related processes. As part of the ECS PCR, the DHS Privacy Office has recommended ways in which NPPD could update the ECS PIA to provide additional transparency to the program and privacy protections that have been implemented. We will review the status of the implementation of those recommendations within one year from the issuance of the PCR. Accordingly, the DHS Privacy Office has no recommendations to include as part of this assessment.

V. EO Section 4(e) Implementation Activity: The DHS Loaned Executive Program

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

As noted in the 2014 Report, the Department plans to leverage the existing Loaned Executive Program⁴¹ to implement Section 4(e) of the Executive Order. During the prior assessment period, preparations were under-way to include private sector cybersecurity experts in the Loaned Executive Program by developing focused cybersecurity-related assignments for prospective participants, and; in last year's assessment, the Department announced its plan to conduct a PIA of the Loaned Executive Programs as a whole.

The Loaned Executive Program is administered by the DHS Private Sector Office and provides an unpaid opportunity for executive-level and subject matter experts from the private sector to share their expertise with DHS. As determined by the DHS components hosting them, the participants are assigned to serve as subject matter experts or senior advisors to DHS leadership, evaluate existing policies, procedures, and training, and/or provide guidance on the public-private partnership model and implementation of strategies designed to improve private sector engagement with DHS.

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

During this reporting year, the DHS Privacy Office worked with the Private Sector Office to conduct and publish a PIA of the Loaned Executive Program. That PIA is available on the DHS website.⁴²

During the current reporting period, there were no cybersecurity experts onboard DHS through the Loaned Executive Program. We will assess the program in the future, when cyber loaned executives are onboard.

Finally, we renew and slightly expand upon the recommendation we made for the program in last year's report.

Recommendation

The DHS Privacy Office recommends that cybersecurity experts in the Loaned Executive Program receive appropriate privacy training as a condition of participation in the Program, with a particular focus on rules for accessing and handling DHS-held personally identifiable information that the loaned executives may encounter during their appointments. The Privacy Office will provide guidance and assistance to the Program to support development of the privacy training.

VI. EO Sections 9(a) and 9(c) - Identification of Critical Infrastructure at Greatest Risk

Section 9(a) of the Executive Order requires the Department to identify entities where a cyber incident could reasonably be expected to have catastrophic consequences, specifically requiring DHS to:

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.

The Department is also required to use the Consultative Process established under Section 6 of the Order, and to work with Sector Specific Agencies in identifying such entities. In doing so, the Department is to “apply consistent, objective criteria in identifying such critical infrastructure.” Once the list of such entities is identified, the Department is required by Section 9(c) of the Order to confidentially notify the owners and operators of the identified infrastructure, and provide them with the basis for the identification. DHS is further required to establish a process by which owners and operators of critical infrastructure may submit relevant information and request reconsideration of the Department's identification. The list of identified entities is to be reviewed and updated annually, following the same procedures.

The Department's Office of Cyber and Infrastructure Analysis (OCIA) (formerly the Infrastructure Analysis and Strategy Division (IASD)), within NPPD, was assigned responsibility for executing Section 9(a). OCIA is responsible for assessing critical infrastructure and producing analysis to be used by government and critical infrastructure owners and operators. Those analytic products inform the development of policy for strengthening critical

⁴² Available at <http://www.dhs.gov/sites/default/files/publications/dhs-privacy-pia-dhs-all-loaned-executive-program-09292014.pdf>.

infrastructure security and resilience, and support response and recovery efforts during natural, man-made or cyber incidents. The office is experienced in conducting objective analysis of critical infrastructure.

The inquiry to identify cyber dependent infrastructure begins with the threshold question of whether the entity under consideration is truly cyber dependent. Only those entities whose failure *due to a cyber incident* would lead to catastrophic effects are covered.

If an entity is truly cyber dependent (e.g., if its failure due to a cyber incident could not be mitigated by manual workarounds), the inquiry then turns to whether specific types of catastrophic consequences are reasonably foreseeable as a result of the cyber failure. Such consequences may at first appear to be reasonably foreseeable, but if there are substitute goods or services available from elsewhere in the sector which could mitigate the consequences, then the entity does not meet the criticality requirement. For instance, a cyber-dependent manufacturer could suffer a failure due to cyber incident, and that in turn could reasonably and foreseeably cause catastrophic effects. If the entity established processes and procedures to operate its main business functions both on and off-line before the effects occur, however, then the network failure could be mitigated. Similarly, if there were other critical infrastructure owners and operators that could compensate for the loss of those goods and services, thereby preventing catastrophic effects, then the consequences of the cyber-dependent entity's failure could be mitigated. In either instance, the entity would not be classified as a cyber-dependent entity under Section 9(a).

Although the use of the term “catastrophic effects” is somewhat novel in the cybersecurity context, OCIA arrived at the definition of the term by relying upon prior statutory measures and policy work which defined and analyzed the Nation's critical infrastructure. Critical infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.”⁴³ That standard focuses on “debilitating effects,” a threshold that is considerably lower than the “catastrophic effects” standard, because “debilitating effects” is part of how all critical infrastructure is defined, and the effects covered by this definition may be immediate, on the infrastructure itself, or broader, on the national economy or public health. That is a potentially expansive scope, so OCIA framed their interpretation of the Order's requirements more narrowly, focusing on only those cyber-dependent entities whose network failure would likely cause the most grievous or “catastrophic” consequences. To narrow the focus onto the most critical of the cyber dependent infrastructure, OCIA borrowed an analogous definition of catastrophic physical consequences provided in the *9/11 Commission Recommendations Act of 2007* (PL 110-53).

As identified in the Executive Order, three types of catastrophic effects that could result from a failure of cyber dependent infrastructure were considered when OCIA developed a metric⁴⁴ to

⁴³ 42 U.S.C. § 5195c(e)

⁴⁴ The precise criteria used by OCIA for determining what events comprise catastrophic consequences were discussed with the Sector Councils, have been reviewed by the DHS Office for Civil Rights and Civil Liberties and the DHS Office of the General Counsel, and disclosed to the relevant oversight committees in Congress. Those criteria cannot be discussed in detail in this assessment, however, because that information could be used to “reverse

gauge the magnitude of such failures. The types of effects, with the general (paraphrased) standards applied to gauge catastrophic severity include:

- **Public Health or Safety:** high level of deaths, caused promptly by the failure of the cyber-dependent infrastructure;
- **Economic Security:** very large projected economic damages, resulting within one year or less following the event, including costs stemming from business or commerce disruption, evacuation, destruction of wealth or commodities, repair and recovery, and downstream economic costs;
- **National Security:** severe degradation of the Nation's national security capabilities.

The catastrophic effects standard is significant because it provides a uniform standard for determining which entities are covered by Section 9(a). It distinguishes between the physical or economic effects on the entity itself, and focuses on the consequences of a failure as they would be felt from the public health or safety, economic and national security perspectives. Because this standard focuses on objective consequences rather than on the unique economic metrics or inputs and outputs of specific sectors, it can be applied evenhandedly across all sectors, as the economic, geographic and physical variations among critical infrastructure entities in the various sectors are factored out. Only the magnitude and type of consequences should a critical infrastructure entity fail are considered. The catastrophic effects standard also serves an important limiting function on the reach of Section 9(a) activities, clearly defining the scope of the identification and notification process.

To identify entities under Section 9(a), OCIA relied on already-developed critical infrastructure evaluation criteria used by DHS in other critical infrastructure identification activities, developed in response to the *9/11 Commission Recommendations Act* and reflected in the *National Critical Infrastructure Prioritization Program (NCIPP)*. The NCIPP criteria apply a baseline for critical infrastructure consequence analysis that is applicable to any critical infrastructure sector regardless of variations between sectors. This analysis results in an objective prioritization of critical infrastructure across sectors, identifying those entities whose failure would be most consequential. This process does not take into account whether any threat actors are known to be targeting entities identified under Section 9(a), nor does identification under Section 9(a) constitute a finding that the identified infrastructure has inadequate cybersecurity measures in place. Instead, identification as a Section 9(a) entity signifies only that the infrastructure's failure due to a cyber incident could produce catastrophic results, either directly or through identified dependencies and interdependencies in the economy.

The Department began the identification process in spring, 2013 by consulting with many critical infrastructure stakeholders, spanning the nation's critical infrastructure sectors and many critical infrastructure coordinating bodies. The use of the Order's *Consultative Process* (Section 6) permitted OCIA to leverage the expertise of the nation's participating critical infrastructure actors to narrow the in-depth analytic focus onto those sectors and sub-sectors most likely to contain critical infrastructure, the failure of which would be particularly consequential.

engineer" the DHS analysis and determine which CDI entities are considered the nation's most vulnerable points. Nevertheless, some discussion of that analysis is suitable for public disclosure in this context.

Notice concerning the process was sent through the Sector Coordinating Councils and Critical Infrastructure Partnership Advisory Council alerting partners of the working group. The Sector Specific Agencies also reached out directly to critical infrastructure partners where appropriate or when specific expertise was needed from a sector. Public input was possible, and the input from critical infrastructure sector councils, major critical infrastructure actors, subject matter experts and others provided DHS with information about how various sectors functioned, and the possible consequences of disruption in each sector. Further analysis then helped identify those critical infrastructure entities meeting the requirements of Section 9(a). Sector stakeholders were involved consistently in the process.

Stakeholder participation was vital, assisting in the identification of Section 9(a) entities that might otherwise not have been identified. This was particularly true where the effects of a failure would be disproportionately large compared to the size of the critical infrastructure entity; such economic and practical inter-relationships are often difficult to identify for those lacking detailed, every day familiarity with the sector or subsector. OCIA was able to readily identify some large entities that met Section 9(a) criteria based in part on critical infrastructure analysis that had already occurred prior to issuance of the Executive Order, and because some critical infrastructure entities meeting the criteria self-identified and were readily confirmed as meeting the criteria.⁴⁵ But other entities, particularly smaller entities and low-visibility but highly interdependent entities upon which many other critical infrastructure actors depend, were identified only with the assistance of the expert knowledge of stakeholders, Sector Specific Agencies,⁴⁶ regulatory agencies and the Sector Councils.

The identification process allowed for and relied upon substantial stakeholder participation. The DHS employees involved in the identification process and contacted during the fact finding phase of this assessment indicated that the experts and stakeholders operated independently and that no parties to the process sought to improperly influence the inclusion or exclusion of specific critical infrastructure entities. Those employees also indicated that some entities thought at the outset to be among the most likely to be identified under Section 9(a) after deeper consideration and assistance of experts did not meet the 9(a) criteria after all. This evolution occurred when the experts and stakeholders consulted in the interactive process and were able to identify how replacement goods or services would be readily available from other entities within that critical infrastructure sector, or when they ascertained a sector specific mitigation process that was already established to mitigate such a failure. Similarly, some entities that are not

⁴⁵ A critical infrastructure entity can self-identify as a Section 9(a) entity in the same way any critical infrastructure entity can volunteer information to OCIA indicating that it might be cyber dependent infrastructure. OCIA will evaluate the self-identifying entity using the facts provided by the entity, and other facts surfaced through the Section 9(a) identification process. The fact of initial self-identification is not dispositive in the process and interest in being classified as a Section 9 entity does not affect the DHS evaluation.

⁴⁶ Sector Specific Agencies are defined in Presidential Policy Directive (PPD) 21. In that directive, DHS is given the responsibility to “provide strategic guidance, promote national unity of effort, and coordinate the overall effort to protect and ensure the resilience of the nation’s critical infrastructure.” Sector Specific Agencies are those Departments or Agencies which have day to day responsibilities to oversee or regulate specific sectors or subsectors of the critical infrastructure. In the security context, Sector Specific Agencies are required pursuant to PPD-21 to act within their existing statutory and regulatory authorities, and to coordinate with DHS in carrying the critical infrastructure protection mission. In practice, this results in DHS taking the overall lead for coordination, with sector specific agencies leveraging their unique missions and expertise to determine the most effective way to protect critical infrastructure and ensure resilience within their own sector. .

typically or intuitively considered as major critical infrastructure actors were identified as essential lynchpins in the critical infrastructure – cyber-dependent entities whose failure could not be mitigated and which could reasonably result in catastrophic consequences.

By July 19, 2013, the list of entities identified under Section 9(a) was complete for Fiscal Year 2014. It will be reviewed and revised annually as required in the Order, with entities being added to or removed from the list as appropriate. The master list is classified pursuant to national security classification guidelines, commensurate with the damage that could be caused should the list be disclosed publicly or to the Nation’s adversaries. Such disclosure could provide adversaries a targeting list. The identity of any particular entity under Section 9(a) or the fact of its individual inclusion on the master list of identified 9(a) entities, however, is generally unclassified.⁴⁷ Even though these identifications could reasonably have been classified as national security material, few of the identified entities employ individuals who hold security clearances, or have the ability to handle and store classified information. The Department therefore exercised its discretion as an original classification authority and deemed most of the individual identifications unclassified.

Once the list of Section 9(a) entities was completed, the process of notifying the identified critical infrastructure entities began. Notification to identified entities occurs under Section 9(c) of the Executive Order, which requires DHS to:

Confidentially notify owners and operators of critical infrastructure identified under subsection (a) . . . that they have been so identified, and ensure identified owners and operators are provided the basis for the determination.

Along with notification to identified entities, the Department also provided notice of the reconsideration process, which was established pursuant to Section 9’s requirement that the Department “establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications. . . .”

That process was described in detail on April 17, 2014, in a public notice⁴⁸ of a reconsideration procedure permitting critical infrastructure identified on the list, as well as those not on the list, to request reconsideration of their status from the OCIA.

OCIA began notification using certified letters from the Under Secretary, NPPD, to owners and operators of identified critical infrastructure in early February 2014. Most notifications were completed by late February 2014, although a few entities whose identification under Section 9(a) is a classified fact, have still not been provided with written notice of Section 9(a) identification, and are awaiting the issuance of security clearances that will permit the Department and Sector Specific Agencies to candidly discuss the matter with them, and to allow them to retain the written notice and other factual information they would need to facilitate reconsideration, should they so desire. In those instances where the identification as a Section 9(a) entity was classified,

⁴⁷ Some Sector Specific Agencies did ask DHS to apply national security classification to the identification of a few regulated entities within their sectors, seeking classification due to the national security sensitivity of the identification, but by and large the association of individual critical infrastructure entities with this list is not classified.

⁴⁸ FR Doc No: 2014-08702.

notification was conducted in person by DHS officials, and DHS retained a copy of the written, classified notice.

Because most identifications under Section 9(a) are unclassified and have been shared with the identified entities, those entities that did not receive notification by February 2014 can conclude that they were not identified as Section 9(a) entities during fiscal year 2014.

The notification letters were based on a form letter template and tailored to the specific entity, conforming to the Federal Register announcement describing the identification and notification processes, and included information about the reconsideration procedure for those entities that disagreed with being identified, or not identified, under Section 9(a). The notification to identified entities advised that:

- the notification would be held in confidence, consistent with the Executive Order's requirements;
- the infrastructure owner or operator could request reconsideration of the identification and listing;
- the basis for the determination could be provided, and that the analysis did not focus on known threats or cybersecurity posture of the entity, but on the entity's role in the economy; and
- DHS was available to engage in a dialogue to apprise the owner or operator of specific cybersecurity resources and capabilities available throughout DHS and potentially other agencies to assist in developing a fuller risk assessment and evaluating potential mitigation measures.

Some critical infrastructure owners and operators subsequently engaged with DHS to utilize the cybersecurity resources and capabilities offered by DHS and other Federal agencies. Those tools and processes are available to all potentially affected critical infrastructure entities, but they are specifically highlighted for the owners and operators of entities identified under Section 9(a) as an outreach measure, to make them aware of generally available assistance that might be particularly helpful in reducing risk of a network failure of the type likely to lead to catastrophic effects. The only actual incentive for engaging with DHS presently offered in the Executive Order to notified owners and operators is prioritization for consideration in the process of obtaining a security clearance under Section 4(d) of the Executive Order, for purposes of improving classified information sharing related to cyber threats and other threats to the listed entity.

Methodology

1. The data collected and used in this assessment was collected during the course of interviews with program personnel, and reviews of program documents such as briefing decks, summaries of methodologies and program operation, communications templates, and public notice and communications regarding the Cyber Dependent Infrastructure Identification and entities identified and notified of identification under Section 9(a) of the order.
2. Our analysis of the civil liberties impacts of these activities began with a Constitutional and statutory issue-spotting approach, as described in the introduction to the DHS portion of this report. During our fact finding efforts, we determined that constitutional due process

protections, as provided by the Fifth Amendment, was the most relevant guidepost in evaluating these activities. CRCL consulted with the DHS Office of the General Counsel in the establishment of this program and has no concerns about the legal footing of the program. The CRCL analysis therefore focused on program and policy questions, including whether the Section 9(a) identification and notice processes are even-handed, fair, and sufficient to protect the due process rights of the identified entities and the rights of critical infrastructure entities that are not identified under Section 9(a).

Civil Liberties Assessment

Protective Measures. The balanced and objective method of identification of entities under Section 9(a) serves as a protection of the rights of critical infrastructure entities, owners and operators. DHS has the authority and duty under the Homeland Security Act of 2002 to take steps to protect critical infrastructure entities.⁴⁹ The Department must, in accordance with legal, resource and practical limitations, prioritize its efforts and direct those efforts to the most critical portions of the Nation's critical infrastructure: those entities whose failure would have the most serious consequences for public health, the Nation's economy and national security. The Department must do so in a way that does not diminish civil rights and civil liberties.⁵⁰ This includes ensuring that the Department's interactions with critical infrastructure entities comport with due process and fundamental fairness. Several principles that are protective of civil rights and civil liberties are in operation in the identification and notification processes conducted under Section 9 of the EO.

CRCL found the method used for identifying the entities under Section 9(a) is objective, balanced, and fair. It is also consistent with established processes used by DHS in the identification and prioritization of a wide range of other critical infrastructure. In addition to relying on established process, part of the Section 9(a) entity identification effort relied on established facts, developed from previous non-cyber findings by the NCIPP, which identified and evaluated the consequence of loss of much of the nation's most critical physical infrastructure.

Government input was not the only basis for the identification decisions. OCIA displayed openness to facts and judgments from a wide range of sources, and a commitment to follow their independent, objective analytical process to wherever it might lead. During the consultative process, some entities considered likely critical infrastructure entities under Section 9(a), were found to be either capable of mitigation in case of failure, or were not found to be strictly cyber dependent. At the same time, critical infrastructure entities that the program had not considered at the outset were subsequently identified as Section 9(a) entities when the facts merited such determinations. The inclusion of unanticipated analytical results into the final (for 2014) list of entities identified under Section 9(a), an openness to course corrections when merited by the facts, reflects a balance and a receptiveness to stakeholder input, and facts into the deliberative process. For this reason, CRCL found that the process used for identification was fundamentally

⁴⁹ See Section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121 *et seq*; 131 *et seq*; and 1241).

⁵⁰ 6 U.S.C. §111(b)(g)

fair, both in substance and procedurally, as a result of using a process for decision-making that was protective and inclusive of stakeholders.

CRCL also examined the notification process to ensure that it was appropriate. DHS has a statutory duty to protect critical infrastructure but very little authority to compel cybersecurity cooperation in most critical infrastructure sectors. The challenge for DHS is to work with a broad range of critical infrastructure entities in a manner that invites cooperation in the task of improving security, without relying on or attempting to compel cooperation. In order to implement the EO, DHS must therefore work through collaboration, partnerships, and the identification of issues of mutual concern with critical infrastructure owners and operators, to encourage them to take action to protect themselves and those who might be affected by their failure.⁵¹

Engagements with the private sector in the entities identified under Section 9(a) and notification process must therefore proceed with a light touch, displaying transparency, communicating findings and leading in a way that it does not rise to the level of a regulatory action implicating the procedural requirements of the Administrative Procedures Act.⁵² It is essential instead that DHS act in a manner that builds trust, and allows DHS to lead efforts to improve cybersecurity and to encourage entities identified under Section 9(a) to participate, without attempting to compel entities identified under Section 9(a) to engage in the process. CRCL believes that DHS has met this standard in the notification process.

Possible Civil Liberties Risks. A concern for CRCL is that identification and notification could be interpreted as potentially coercive or regulatory, carrying with it consequences for identified entities. Although most notified entities were not surprised by DHS identifying their consequentiality under Section 9(a), some were surprised. The surprise of receiving a notification of Section 9(a) identification could cause an entity to consider changing how it operates and impel it to invest significantly in strengthening its cybersecurity posture, or to take other actions in response to DHS findings. An entity might be concerned about the potential reputational harm and loss of good will if confidentiality is breached and the entity is publicly identified as one of the Nation's most consequential cyber-dependent entities. It may also be concerned whether the notification highlights some weakness in its cybersecurity posture or imposes some duty of care. Notification thus could conceivably have implicit adverse effects on those entities identified under Section 9(a), including adverse effects on corporate and individual rights and interests. This possibility means that it is important that the analysis is based on facts, free of bias, accurately convey the significance of Section 9(a) identification in a measured manner, and be no broader in scope than necessary, focusing only on those entities which occupy a lynchpin position within the Nation's critical infrastructure.

⁵¹ See E.O. 13636; Presidential Policy Directive 21; and Section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121 *et seq*; 131 *et seq*; and 1241).

⁵² This does not speak to the extent of the authorities of the Sector Specific Agencies or the independent regulatory agencies with which DHS consults in protecting critical infrastructure. Some of those agencies *may* have authorities that allow the regulation of some aspects of cybersecurity within their respective sectors. That is a matter for those agencies to work through and beyond the scope of this Assessment.

Protective Measures in the Process. OCIA personnel reported to CRCL that despite the presence of several hundred stakeholders in this process, and cyber incidents being a prominent issue in the media and politically, they experienced no improper external pressure to include or exclude any entities from the list of entities identified under Section 9(a). They believed this helped them complete the identification process in an objective manner, and free from actual or apparent external bias. Once the analysis was complete, a very small portion of the critical infrastructure in the Nation was identified as covered by Section 9(a). While the total number of entities identified is not appropriate for public disclosure, the number (in comparison to the total number of critical infrastructure entities in the Nation) is statistically insignificant, reflecting a very small DHS footprint.

There are four specific ways in which the Section 9 identification and notification procedures avoid harming, and serve to protect, the subject critical infrastructure entities.

- 1) **Confidential identification and notification do not harm entities identified under Section 9(a).** The notification letter template makes it abundantly clear that the notification is related only to the entity's position in the critical infrastructure, that identification under Section 9(a) is not a finding of flaws in the entity's cybersecurity posture, nor a finding of direct threats posed to the identified entity, and it is confidential. Whatever duty the entity had to mitigate those types of threats or if it has such a duty at all – an open and almost entirely unexplored legal question beyond the scope of this Assessment – is likely unchanged by this notice.

The Department also takes appropriate steps to avoid reputational harm and subsequent loss of commercial good will to entities identified under Section 9(a). The master list of identified entities is maintained as national security information, stopping one way in which the identities of these critical infrastructure actors could suffer reputational harm, and the individual entities' identities are not publicly disclosed by DHS. Additionally, the Protected Critical Infrastructure Information (PCII) program shields the confidentiality of any data the entities identified under Section 9(a) choose to share with the Government, if the entity requests such protection. When an entity has requested confidentiality through the PCII "categorical exemption," its communications to the government are held in confidentiality, and shielded where legally appropriate from other disclosures, such as under the Freedom of Information Act (FOIA) and in certain civil litigation contexts. These are not ironclad guarantees that the notification and reconsideration request will not be disclosed, but they provide good faith assurances of protection while permitting notification of entities identified under Section 9(a), and to provide a fair reconsideration process that does not require the entities to undertake additional reputational risk.

The alternative to notification – that DHS perform its routine mission to identify critical infrastructure but then keep the identities of those entities internal to DHS and refrain from informing the entities of the risk associated with their position in the nation's critical infrastructure – could be viewed as a breach of the Department's duty to protect. Should an adversary cause a network failure at an identified Section 9(a)

entity, with corresponding catastrophic consequences, DHS's actions could plausibly be viewed as unconscionable and a failure to prospectively notify at-risk critical infrastructure. An entity receiving notice of Section 9(a) identification may be aware of the full implications and may have hardened itself to cyber attack, or it may be unaware of the risks and in need of information and technical assistance to reduce its, and the Nation's, vulnerability. Given the threat landscape and the reasonably foreseeable consequences should an identified entity fail, withholding notification of Section 9(a) identification is simply not a plausible alternative course of action for the Department.

- 2) **The identification and notification process are not arbitrary.** The identification and notification process do not function arbitrarily; they are driven by objective facts and informed opinions of those who work in the identified sectors, and both experts and the public have the opportunity to comment through the Consultative Process. The notice published by the Department concerning the Section 9(a) identification process indicates that the Department will make the facts and rationale for the listing available to identified entities upon request, to help them understand why they were identified under Section 9(a) and to provide them with information and directions to facilitate their use of the reconsideration process.
- 3) **The notification process is not a regulatory action.** The notification process does not amount to a regulatory action that would pressure the entity into working with the government. Publicly releasing the information that an entity's network failure could result in catastrophic harm could cause serious reputational harm to the entity, and the possibility of that release could conceivably be used to pressure the entity into cooperation. The Department's measures to preserve confidentiality, however, are meant to ensure that the notification process does not bring public pressure to bear on the entities identified under Section 9(a), and the notification itself makes it clear that any further engagement with DHS and the U.S. Government is voluntary on the part of the entity. This assurance applies whether or not the entity chooses to engage further with the Department, and it reduces the possibility that the fact of notification might be misinterpreted as a regulatory act, one involving a quiet, implicit threat of publication.
- 4) **There is a reconsideration process if the entity believes the identification was wrong or unfair.** Finally, the Department provided a reconsideration process. Those entities identified under Section 9(a) that disagree with their identification can seek reconsideration using a process described in the Federal Register. Like other aspects of the process, the request for reconsideration would be maintained in confidentiality by the Department, and only DHS, and, if appropriate, the relevant Sector Specific Agency, would be aware the reconsideration request had been made. Any critical infrastructure entity that feels it has been harmed by an incorrect identification may use this process to seek redress. Those notified of their identification under Section 9(a) are apprised in the notification letter that the Department will make the facts and rationale for their identification available upon request. If the entity disagrees with the

identification, they may then use those facts, and submit other facts to the Department, and request reconsideration of the identification.

The same reconsideration process is open to *any* U.S. critical infrastructure entity whose owner or operator believes that their identification under Section 9(a) (or lack thereof) is erroneous. Those entities that do not receive notification can utilize the same process to obtain reconsideration. This does not guarantee that the result will change, but since the identification is the result of multiple processes, including consultation with affected entities, OCIA is open to new facts and including, or removing an entity from the list of Section 9(a) entities, as appropriate, if the entity seeking reconsideration provides facts showing such action is appropriate.

When a reconsideration process is allowed as part of final decision-making, it is generally treated as a method of providing procedural due process for those affected by a decision. CRCL believes that the reconsideration process, in which DHS is committed to explaining the reasoning behind its decision to identify, or not identify, a particular entity, will work to enhance the fairness and objective accuracy of Section 9 identification, and will not convey an unfair advantage on those entities identified under Section 9. Even though a reconsideration process is not required here, it utilizes common due process-protecting measures and serves as an additional procedural protection of the rights and interests of potentially affected critical infrastructure entities.

PART II: DEPARTMENT OF THE TREASURY



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 November 15, 2013 to September 30, 2014 reporting period.

1. Summary description of agency 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.

2. Summary/overview of 13636-relevant activities to be assessed

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.

3. 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 personally identifiable information (“PII”).

4. Detailed analyses of implementation activities under EO 13636 to be reviewed

- a. **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.*

- i. Detailed description of activity

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 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.

ii. 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 conducting 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 2014 Executive Order 13636 Privacy and Civil Liberties Assessments Report.

Treasury uses 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.

In fiscal year 2015, Treasury plans on developing a cybersecurity analysis based upon comments received from the Privacy and Civil Liberties Oversight Board. Due to time constraints and issues associated with the

unique organizational structure of Treasury, this type of analysis could not be performed in the time allotted for this assessment period.

iii. PCL assessment

1. PCL protections within activity; PCL 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 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.
Please describe any steps taken to mitigate any use of PII that is not specified in the applicable notices.	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

Protections	Response
	local folder, with access limited to only those who have a need to know the information to perform their duties.
<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 maintained within the system?</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 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.</p>
<p>Please describe any agency oversight mechanisms that apply to the system.</p>	<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</p>

Protections	Response
	<p>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>

2. PIAs or other documentation, as appropriate

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.

3. FIPPS and/or Civil Liberties analysis, as appropriate:

Transparency	Response
<p>How is the general public informed about the DHS Critical Infrastructure Private Sector Clearance Program?</p>	<p>DHS is the lead agency for the DHS Private Sector Clearance Program. Pursuant to the E-Government Act of 2002 and 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.</p>
<p>When collecting information from members of the public, does the program submit documentation for an OMB Collection number?</p>	<p>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.</p>
<p>Does the agency operate a Privacy Act system of records in support of the DHS Critical Infrastructure Sector Clearance Program?</p>	<p>Treasury does not operate a Privacy Act system of records in support of the DHS Private 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</p>

Transparency	Response
	information.
<p>How does this program ensure that notices are updated to reflect system or program changes?</p>	<p>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.</p>

Individual Participation	Response
<p>Are individuals asked for consent and given the opportunity to object to the collection of their PII?</p>	<p>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 refusal to submit the information will result in their inability to secure a clearance.</p>
<p>Are individuals given the opportunity to access and correct their PII?</p>	<p>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.</p>
<p>Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or</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 Treasury Directive (TD), 25-08, <i>Safeguarding Against and</i></p>

Individual Participation	Response
disclosure of their PII.	<i>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 PPD 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
Please describe the data elements that are relevant and necessary.	<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 utilized 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 Clearance 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 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.</p>
<p>Please describe the method for eliminating PII that is no longer needed.</p>	<p>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.</p>

Security	Response
<p>Please describe any safeguards that are in place to ensure the continued security of data maintained within the system.</p>	<p>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.</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 and audit controls to prevent unauthorized access to or use of data at rest on the DO LAN.</p>
<p>If data from the system is sent electronically, what methods are in place to ensure appropriate safeguards apply?</p>	<p>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.</p>

Accountability and Auditing	Response
<p>What methods are in place to audit access to records maintained within the system?</p>	<p>Treasury 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>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</p>

	operations or when it has been previously assessed under an evaluation similar to a PIA.
--	--

Civil Liberties Considerations
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.

4. PCL risks/impacts:

Risk	Impact
Please explain the possibility of redress if data loss due to an email breach.	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.
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.

5. Broader PCL issues, policy considerations, and legal considerations raised:

None

iv. Recommendations:

None

v. Issues for future tracking and evaluation:

Per the Privacy and Civil Liberties Oversight Board’s comments, a more thorough privacy assessment may be conducted in future reports.

b. Section 4(a) Information Sharing: *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.*

(i) Detailed description of activity:

To increase the volume, timeliness, and quality of cyber threat information shared with U.S. financial sector entities so that these entities may better protect and defend themselves against cyber threats Treasury requests declassification of and subsequently disseminates relevant law enforcement and intelligence information. Through a consultative process required by EO 13636, Treasury assists law enforcement and national security agencies with identifying critical infrastructure where a cybersecurity incident could reasonably result in catastrophic consequences. Following the consultation, DHS directly notifies owners and operators of the critical infrastructure identified as being at a great risk. During the previous reporting period, Treasury began to identify appropriate points of contact for critical infrastructure vulnerabilities identified under this section. Treasury continued to receive cyber threat information from the private sector in the current reporting period.

ii Description of assessment methodology:

See description in section 4(d).

iii. PCL assessment

1. PCL protections within activity; PCL compliance:

Information in this program is only disseminated to private organizations with a need to prevent Financial Services Sector breaches.

2. PIAs or other documentation, as appropriate:

Information in this program is disseminated through correspondence. Treasury’s non-classified electronic mail 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.

3. FIPPs and/or Civil Liberties analysis:

Transparency	Response
How is the general public informed about this program?	The general public is informed of this program through PPD 21.
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 record 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?	Treasury is not responsible for the collection of PII in this program and therefore is not required to ask for consent.
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 should 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 PII in the form of IP addresses. As part of its information sharing activities under 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.	Treasury does not collect information 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.

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 private sector by electronic means. The dissemination is limited by the Traffic Light Protocol and includes a statement that the information is “NOT FOR POSTING ON ANY PUBLIC-FACING WEBSITE.”

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.

4. PCL risks/impacts:

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.

5. Broader PCL issues, policy considerations, and legal considerations raised:

None

iv. Recommendations:
None

v. Issues for future tracking and evaluation:

Per the Privacy and Civil Liberties Oversight Board's comments, a more thorough privacy assessment may be conducted in future reports.

c. 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 unwarranted.

5. Summary of findings and recommendations:

Treasury plays a minor role in disseminating PII in two programs. At this time, there are few improvements that need to be made to both programs because of this limited role. The possibility of these improvements relies heavily on the development of new technology.

6. Conclusion:

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, and then may nominate them for national security clearances.

Through a consultative process developed by EO 13636, Treasury assists law enforcement and national security agencies with identifying critical infrastructure where a cybersecurity incident could reasonably result in catastrophic consequences. Treasury also identifies cyber threat information collected by law enforcement and intelligence agencies that is relevant to the Financial Services Sector, requests declassification of that information, and once declassified distributes this information to the sector for use in network defense. In all three programs, Treasury plays a minor role in the dissemination of PII. In the future, Treasury plans to continue its work in these programs to assist in the dissemination of cybersecurity information while protecting privacy and civil liberties.

PART III: DEPARTMENT OF DEFENSE



I. INTRODUCTION

The Department of Defense (DoD) submits this privacy and civil liberties assessment for inclusion in the 2015 Executive Order 13636 Privacy and Civil Liberties Assessments Report. This assessment revises DoD's submission to the 2014 report.

The Defense Privacy and Civil Liberties Division (DPCLD)

The mission of the DPCLD is to implement the DoD Privacy and Civil Liberties Programs through advice, monitoring, official reporting, and training. In discharging its assigned responsibilities, the DPCLD assists the DoD Senior Agency Official for Privacy, the DoD Civil Liberties Officer, and DoD Components to appropriately consider privacy and civil liberties in all programs and initiatives.⁵³

DoD Privacy Program⁵⁴

The DoD Privacy Program provides a comprehensive framework regulating how and when the Department maintains⁵⁵ personally identifiable information (PII)⁵⁶. The purpose of the DoD Privacy Program is to balance the information requirements and needs of the Department with the privacy interests and concerns of the individual.

The DPCLD performs multiple functions to facilitate Department-wide compliance with the DoD Privacy Program, to include:

- Developing policy, providing program oversight, and serving as the DoD focal point for Defense privacy matters;
- Providing policy guidance and assistance to the DoD Components in their implementation and execution of their privacy programs;
- Reviewing new and existing DoD policies which impact on the personal privacy of the individual;
- Reviewing, coordinating, and submitting for publication in the Federal Register Privacy Act System of Records Notices (SORN) and Privacy Act rulemaking by the DoD Components;
- Developing and coordinating Privacy Act Computer Matching Programs within the DoD Components and between the DoD Components and other federal and state agencies;
- Providing administrative and operational support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee; and

⁵³ The Deputy Chief Management Officer of the Department of Defense serves as both the DoD Privacy and Civil Officer and the Senior Agency Official for Privacy and reports directly to the Secretary of Defense.

⁵⁴ The DoD Privacy Program is based on the Privacy Act of 1974, as amended (5 U.S.C. 552a), as implemented by Office of Management and Budget (OMB) Circular A-130 "Management of Federal Information Resources," February 8, 1996, and DoD regulatory authorities DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, as amended, and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

⁵⁵ See 5 U.S.C. 552a(a)(3). The term "maintain" includes maintain, collect, use, or disseminate.

⁵⁶ The term "PII" is defined in OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007.

- Developing and administering Privacy Act training and awareness materials for all DoD Components.

DoD Civil Liberties Program⁵⁷

The DoD Civil Liberties Program establishes DoD policy to protect the privacy and civil liberties of DoD employees, members of the Military Services, and the public to the greatest extent possible, consistent with the DoD's operational requirements.

The DPCLD helps ensure Department-wide compliance with the DoD Civil Liberties Program by:

- Developing policy, providing program oversight, and serving as the DoD focal point for Defense Civil Liberties matters;
- Providing assistance to the DoD Components to aid the development of component civil liberties programs and incorporation of civil liberties into their activities and initiatives;
- Reviewing new and existing DoD policies for adequate civil liberties protections;
- Collecting and compiling DoD Component reports of alleged civil liberties violations into a DoD report for review by the U.S. Congress and the Privacy and Civil Liberties Oversight Board;
- Supervising and overseeing the activities of the Defense Civil Liberties Board; and,
- Developing and administering civil liberties training and awareness materials for all DoD Components.

Executive Order 13636, Section 5

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"⁵⁸, 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. Specifically, the Order calls for federal departments and agencies to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities. Section 5 requires senior agency officials for privacy and civil liberties to incorporate privacy and civil liberties protections into such activities, and to conduct assessments of those activities, based upon the eight Fair Information Practice Principles (FIPPs) and other applicable policies, principles, and frameworks. Section 5(b) adds that assessments "shall be reviewed on an annual basis and revised as necessary."

⁵⁷ The DoD Civil Liberties Program is based on Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007" (42 U.S.C. 2000ee, ee-1), as implemented by DoD Instruction 1000.29, "DoD Civil Liberties Program," November 26, 2014. See <http://www.dtic.mil/whs/directives/corres/pdf/100029p.pdf>.

⁵⁸ See <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

Defense Industrial Base (DIB)⁵⁹

The DIB is 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. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other federal agencies. Defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations.

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

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

To execute its responsibilities for the DIB successfully, DoD must engage in ongoing activities to build trust with DIB critical asset owners and operators to support two-way information sharing and to maintain meaningful relationships and frequent dialogue across the diverse array of DIB stakeholders. Private-sector critical infrastructure program participation is voluntary. Many large size defense industry firms place a great deal of emphasis on protecting their physical, human, and cyber assets. On the other hand, many of the medium and smaller size businesses are challenged to make the capital investments required to perform vulnerability assessments and build resiliency into their operational capabilities.

⁵⁹ See *partnering*, <http://policy.defense.gov/OUSDPoffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram/Partnering.aspx>

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

The DIB CS/IA Program is designed to improve DIB network defenses and allows DIB companies and the government 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. The DIB CS/IA Program is open to all eligible DIB companies. Currently, there are more than 100 companies participating in the program. There have been no policy changes to the DIB CS/IA Program since 2013. Accordingly, the privacy and civil liberties protections associated with this program and assessed in the 2014 report remain the same.

The DIB Enhanced Cybersecurity Services (DECS) is a joint activity with the Department of Homeland Security (DHS), falling under the umbrella of DHS' Enhanced Cybersecurity Services (ECS) program, part of the DHS-led effort to protect U.S. critical infrastructure. DECS is an optional component of the DIB CS/IA Program.⁶⁰

Under the DIB CS/IA Program, DoD provides participating DIB companies with unclassified cyber threat indicators and related classified contextual information. DIB companies can choose whether to incorporate the indicators into their own network traffic screening or other security tools and use the contextual information to better understand the cyber security threats they face. DoD also shares mitigation measures to assist DIB companies' cyber security efforts.

Participating DIB companies agree to report any cyber incidents they discover on their networks that have resulted in an actual or potential compromise of DoD information, and may also, at their discretion, report any other cyber event that may be of interest to the government or the DIB cyber community for cybersecurity purposes. DIB companies may participate in cyber intrusion damage assessments when such assessments are required. The electronic media provided by the participating DIB company is analyzed in support of damage assessments to determine the impact of compromises on DoD programs.

⁶⁰ A detailed analysis of privacy and civil liberties protections contained in the ECS Program is available in DHS' submission to this report. The ECS PIA, DHS/NPPD/PIA-084, "Enhanced Cybersecurity Services (ECS)," is available on the DHS Privacy Office's website at http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf

DIB CS/IA Program and Personally Identifiable Information

The criteria for maintaining PII in the DIB CS/IA Program is whether the PII is relevant and necessary for the authorized program purposes. This means that the DIB CS/IA Program limits the maintenance of PII to that which is relevant and necessary to the analysis of a cyber intrusion incident or follow-on forensic analysis. There are two types of PII involved with the program: (1) DIB company Point of Contact (POC) PII and (2) PII embedded⁶¹ in information collected as a result of electronic transmission or other data collected responding to a cyber-incident, including analysis.

- **POC PII for program administration and management purposes.** DIB companies share with DoD typical business contact information for its personnel that are serving as company POCs for DIB CS/IA Program activities or specific cyber incidents. This PII is limited to the individual's contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone number), along with other information (e.g., security clearance, citizenship) that is necessary to verify the individual's authorization to receive classified or other controlled unclassified information under the program. This information is covered by the Privacy Act Statement (PAS), the program's System of Records Notice⁶² (SORN), and Privacy Impact Assessment⁶³ (PIA).
- **PII embedded in information collected for cyber incident response and analysis purposes.** Although it is not typical or expected, there exists the potential that information provided by a DIB company regarding a specific cyber incident may include PII that is embedded in information being shared for cyber security analysis.⁶⁴

Embedded PII is shared with DoD only if the DIB company determines that the PII is relevant and necessary to the incident response and analysis, and that there are no legal, contractual, or other restrictions on sharing the PII with the U.S. government. This includes a DIB company report that may contain embedded PII as part of a cyber threat indicator (e.g., email address), where the DIB company must determine that the information is relevant to the cyber incident reported and necessary to understand the threat.

The Incident Collection Form used by a DIB company to report cyber incidents to DoD also protects PII by asking the DIB company at the end of each section of the Form if PII is included.

⁶¹ The DIB CS/IA PIA uses the term "inadvertent" PII to define PII embedded in data collected for cyber incident response and analysis purposes. For purposes of this assessment, "embedded" PII is preferred to clarify that any PII collected by DIB companies when responding to a cyber incident, however atypical or unexpected, is the result of an intentional collection that may provide a key element of cyber threat information. The DIB CS/IA PIA is available at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

⁶² See SORN at <http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570553/dcio-01.aspx>

⁶³ See PIA at http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

⁶⁴ See Final rule at <http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf>. To participate in the DIB CS/IA Program, the DIB company must own or operate an unclassified information system that processes, stores, or transmits DoD information.

If the DIB company selects “yes,” DoD is alerted to the presence of PII that must be protected in accordance with the Program’s established procedures to ensure compliance with applicable Federal law, regulations, and policies.

The DIB CS/IA Program is governed by Title 32 of the U.S. Code of Federal Regulations, Part 236, “Department of Defense (DoD) – Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities,” which requires that “DoD and DIB participant will conduct their respective activities in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data [, and that] the Government and the DIB participant[s] each bear responsibility for their own actions under the mandatory reporting requirements.”⁶⁵ In addition, Part 236 requires that, “[p]rior to sharing any information with the Government under this program..., the DIB participant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements.”⁶⁶ All DIB companies must agree to the requirements in Part 236 to be eligible to participate in the DIB CS/IA Program.⁶⁷

The DIB CS/IA Program’s PIA details how DoD and DIB companies will appropriately maintain PII, including PII embedded in information shared for cyber security analysis.⁶⁸ The DIB CS/IA Program Office is reviewing the language in the PIA to further clarify and reinforce appropriate handling and safeguarding requirements and procedures as a prerequisite to maintaining any PII.

⁶⁵ See 32 C.F.R. 236.6(b), at <http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf>

⁶⁶ See 32 C.F.R. 236.6(c), at <http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf>

⁶⁷ See 32 C.F.R. 236.4(a) and (b); see also <http://dibnet.dod.mil/staticweb/Register.html>

⁶⁸ See, e.g., PIA at section 2g(2), “when the DoD is performing its analysis on files, it may discover PII (or other sensitive information) that had not been identified by the DIB company when the information was submitted. If this occurs, all investigative work involving that PII ceases, the DIB company is notified that the PII (or sensitive information) was discovered, and the DIB company provides guidance as to the disposition of that information.”

II. PRIVACY ASSESSMENT

The Fair Information Practice Principles (FIPPs)

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

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

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

1. Transparency	Response
<p>How is the general public informed about the DIB CS/IA Program and information collection?</p>	<p>The public is informed about the DIB CS/IA Program and information collection in the following:</p> <ul style="list-style-type: none"> • The DIB CS/IA Program SORN is DCIO 01, “Defense Industrial Base (DIB) Cyber Security/Information Assurance Records.” The SORN informs the public about the collection, maintenance, and use of information about an individual, where the records can be retrieved by the name of the individual or by some other type of identifier unique to the individual.⁶⁹ • The DIB CS/IA Program PIA.⁷⁰ The PIA assesses the impact on privacy for systems that collect PII. • The DIB CS/IA Program is governed by 32 C.F.R. Part 236, “[DoD-DIB] Voluntary Cyber Security and Information Assurance (CS/IA) Activities,” which is subject to Federal rulemaking procedures, including publication for public comment.⁷¹ <p>In addition, there is a PAS provided to each DIB company POC at the point of collection for the POC PII.</p>
<p>For collections involving PII, how do affected individuals receive notice regarding the maintenance⁷² of their PII?</p>	<p>For the POC PII, affected individuals receive notice in the following ways:</p> <ul style="list-style-type: none"> • The DIB CS/IA Program SORN DCIO 01⁷³ identifies whose information is collected, the types of information collected, the purpose for the collection, routine uses of the information, how it is retrieved, and what safeguards are in place. • The DIB PIA states, “When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she is provided with the opportunity to consent or not consent to specific uses of PII when they are presented with the Privacy Act Statement.”⁷⁴

⁶⁹ See SORN.

⁷⁰ See PIA.

⁷¹ See Interim rule.

⁷² See 5 U.S.C. 552a(a)(3). The term “maintain” includes maintain, collect, use, or disseminate.

⁷³ See SORN.

⁷⁴ See PIA at section 2j(1).

1. Transparency	Response
	For PII embedded in collected information for cyber incident response and analysis purposes, notification may be difficult. In the case of a DIB company employee, the company would be responsible for notifying the employee. However, notice may not be possible if the individual is not a member of the reporting DIB company, is the adversary, or is fictitious.
How does the DIB CS/IA Program ensure that notices are updated to reflect system or program changes?	The DIB CS/IA Program SORN was published in May 2012. DoD SORNs are reviewed every two years. The interim final rule for the DIB CS/IA Program ⁷⁵ was published in May 2012. The final rule ⁷⁶ for the program was published in October 2013.
Is the PIA summary available to members of the public on the DIB or DoD website?	Yes, the DIB CS/IA Program PIA summary is available to the public on the DoD website. ⁷⁷
Does the DIB CS/IA Program maintain an accounting of disclosures made to non-DoD individuals from the applicable system of records ⁷⁸ ?	Yes, DoD will obtain permission from the individual in writing before disclosing information to a non-DoD individual.
Please describe any barriers to ensure continued transparency of the program and its maintenance of PII.	32 C.F.R. Part 236, “Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities,” ⁷⁹ provides general information about the program. It points out that “Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this program against unauthorized public disclosure by asserting applicable FOIA exemptions and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.”

⁷⁵ See Interim Final Rule at <http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf>.

⁷⁶ See Final Rule at <http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf>

⁷⁷ See PIA.

⁷⁸ See 5 U.S.C. 552a (a)(5). A system of records is a group of records under the control of a DoD Component from which PII about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, unique to the individual.

⁷⁹ See 32 C.F.R. Part 236, <http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf>

1. Transparency	Response
When collecting information from members of the public, does the program submit documentation for an OMB Collection number? If so, please provide the OMB Collection Number.	Yes, there are two OMB Control Numbers for the DIB CS/IA Program, 0704-0490 (POC PII) and 0704-0489 (CS/IA Cyber Incident Reporting). ⁸⁰

⁸⁰ See, e.g., the publication for comment of the information collections, at <http://www.gpo.gov/fdsys/pkg/FR-2013-08-30/pdf/2013-21234.pdf>.

2. Individual Participation	Response
<p>Are individuals asked for consent and given the opportunity to object to the collection of their PII?</p>	<p>Yes, the DIB CS/IA PIA states, “When the DIB company POC information is intentionally collected directly from an individual who is being designated as a POC, he/she can object to the collection of PII at that time.”</p> <p>32 C.F.R. Part 236 also states that the confidentiality of information exchanged under the DIB CS/IA Program will be protected to the maximum extent authorized by law, regulation, and policy. DoD and DIB companies each bear responsibility for their own actions under the voluntary program.</p> <p>The DIB company selects individuals to participate as designated points of contact for the DIB CS/IA Program and for the submission of cyber incident reports. The DIB company should afford the individual the opportunity to object to providing such information to DoD.</p> <p>In cases where PII may be embedded in a cyber incident report, the DIB company is asked to identify if PII is included in the report. If the DIB company deems that PII is relevant and necessary in a cyber incident report, then it is the responsibility of the DIB company to ensure that the company is authorized to collect and share that PII with DoD (e.g., through notice and consent of the employee). DoD does not have direct access to contact the individual to enable that individual to object. In many cases, authorized users of a DIB company network are under notice (e.g., policy, banner) that information and data on the network may be monitored or disclosed to third parties, and/or that the network users’ communications on the network are not private.</p>
<p>Are individuals given the opportunity to access and correct their PII?</p>	<p>Yes, the DIB company is responsible for providing updates and corrections as necessary. It is the reporting company’s responsibility to ensure the accuracy of reported information.</p>
<p>Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or disclosure of their PII.</p>	<p>The DIB CS/IA SORN states, “The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 C.F.R. Part 311; or may be obtained from the system manager.”</p>
<p>What steps are taken to ensure information maintained in the system is</p>	<p>DIB CS/IA Program staff periodically review the data and it is incumbent upon the DIB company to provide accurate and updated POC information.</p>

2. Individual Participation	Response
accurate, timely, relevant, and complete?	
Is the provision of PII mandatory or voluntary? If mandatory, please cite the specific policy or guidance that requires the collection as well as rules and outcomes for failing to provide information.	<p>For the POC PII, the disclosure is voluntary. The program’s PAS says, “However, failure to provide requested information may limit the ability of the DoD to contact the individual or provide other information necessary to facilitate this program.”</p> <p>For the disclosure of embedded PII, although not typical or expected, if the DIB company determines that PII is relevant and necessary for the analysis of a reportable cyber incident, then they may include that PII in the report (and the form requires the submitter to identify that PII is included in the report).</p>
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>For POC PII, a DIB company POC provides the information about all of the company’s POCs. As part of the administrative management of the DIB CS/IA Program, each participating DIB company provides basic identifying information for a limited number of its personnel who are authorized to serve as the primary company POCs. The information provided for each POC includes business contact information (e.g., name, title, organizational unit, business email and phone), plus additional information necessary to verify the individual’s authorization to receive classified information or controlled unclassified information (e.g., security clearance, citizenship). This information is required by the DIB CS/IA Program office to manage the program and interact with the companies through routine emails, phone calls, and participation in periodic classified meetings. A DIB company that is not yet participating in the program may also provide POC information to the DIB CS/IA Program office in order to discuss the program, including application procedures or to receive information about the program.</p> <p>Any PII embedded in information for cyber incident response and analysis purposes is not collected from the individual (unless purely by coincidence the PII involved happens to identify the POC that is submitting the report). It is provided only by authorized DIB company POC(s), regarding a specific cyber incident. Any PII embedded in the information is shared only for cyber security analysis.</p>

3. Purpose Specification	Response
<p>Please provide the specific purpose(s) for the maintenance of PII within the system.</p>	<p>The DIB CS/IA Program SORN states: “To facilitate the sharing of DIB CS/IA cyber threat information and best practices to DIB companies to enhance and supplement DIB participant capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. When incident reports are received, DoD Cyber Crime Center (DC3) personnel analyze the information reported for cyber threats and vulnerabilities in order to develop response measures as well as improve government and DIB understanding of advanced cyber threat activity. DoD may work with a DIB company on a more detailed, digital forensics analysis or damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information.”</p> <p>Further DIB CS/IA Program PAS states, “Purpose: Administrative management of the DIB CS/IA Program's information sharing activities. Personal information is discussed in SORN DCIO 01.”⁸¹</p>
<p>What steps are taken to ensure the authority for the collection is valid?</p>	<p>Authority is provided for by 32 C.F.R. Part 236.⁸²</p>

4. Data Minimization	Response
<p>Please describe the data elements that are relevant and necessary.</p>	<p>The DIB CS/IA PIA lists the following POC PII: name, citizenship, security clearance, business email, and business telephone number.</p> <p>Although it is not typical or expected, there exists the potential that information provided by a DIB company regarding a specific cyber incident may include PII that is embedded in the information being shared for the cyber security analysis. If PII is included in a cyber incident report, DoD handling procedures are designed to ensure that PII and other sensitive information is shared by DoD only after the submitting DIB company has determined that the information is relevant and necessary to the analysis of a cyber intrusion incident or follow-on forensic analysis, and that the information has been</p>

⁸¹ See SORN.

⁸² See 32 C.F.R. Part 236, which cites its authority as 10 U.S.C. § 2224, 44 U.S.C. § 3506, and 44 U.S.C. § 3544. Note that 44 U.S.C. § 3544 has been superseded by 44 U.S.C. § 3554 (via the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, December 18, 2014).

4. Data Minimization	Response
	<p>lawfully collected and is authorized for sharing with the DoD. DoD and DIB companies share information about cyber incidents in order to help others know what to look for to prevent a cyber incident or to search for similar activity on a network. If PII is relevant to cyber threat activity and necessary to identify that threat activity, it can be shared. If the PII is not deemed relevant and necessary, it will not be shared. DoD can share cyber incident information including PII with law enforcement/counter intelligence for the purposes of supporting an investigation and prosecution of any individual or organization when the information appears to indicate activities that may violate laws, including those attempting to infiltrate and compromise information on a DIB company information system. Such dissemination must comply with the Privacy Act and all other applicable statutes, regulations, and DoD policies.</p>
<p>Please describe how the program removes data that is no longer necessary for the system.</p>	<p>The DIB company POC information provided to support the DIB CS/IA Program administration and management process is maintained only as long as the designated POC(s) continues to represent the participating company. When the DIB CS/IA Program office is notified that a DIB company POC was replaced, the POC information is updated and outdated PII is archived in accordance with applicable records management requirements.</p> <p>Any PII embedded in information collected by DIB companies that is deemed unnecessary for subsequent analysis is purged. Embedded PII determined to be relevant is maintained and controlled, and subsequently is disposed of when no longer reasonably necessary for cyber incident investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes).</p>
<p>Are records maintained in accordance with National Archives and Records Administration retention and disposal schedules? If so, please describe any applicable schedules.</p>	<p>The DIB CS/IA PIA states, “In accordance with NARA regulation and 32 C.F.R. Parts 1220-1239, program records are retained for a minimum of three (3) years, and tracking/ticketing system records are retained for a minimum of two (2) years.” The final disposition of the retention and disposal schedule is pending with NARA.</p>
<p>Please describe the method for ensuring that only the minimum necessary amount of data is collected.</p>	<p>The information sharing activities covered by the DIB CS/IA PIA are focused on sharing cyber security related information, and the program seeks to minimize the collection and maintenance of PII except as necessary to support the program. The operational</p>

4. Data Minimization	Response
	<p>implementation of this sharing arrangement involves sharing and managing PII in two ways:</p> <ul style="list-style-type: none"> -For program administration and management purposes, the DIB companies share with DoD typical business contact information for its personnel who are serving as company POCs for the program. -For cyber incident response and analysis purposes, although it is not typical or expected, there exists the potential that information provided by a DIB company regarding any specific cyber incident may include PII that is embedded in the information being shared for cyber security analysis. This information is shared with DoD only if the DIB company determines that the PII is relevant and necessary to the incident response and analysis. DC3 analysts review reported data for PII before sharing anonymized report information with other DIB companies and DoD. Information deemed irrelevant and unnecessary for subsequent analysis is purged from DC3 systems. DIB companies also are asked to review information to be shared with other DIB companies and DoD.
5. 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>The DIB CS/IA Program collects DIB company POC PII only for routine program administration and management purposes. This PII does not involve any particularly sensitive personal information – it is limited to the individual’s contact information that is routinely shared in the ordinary course of business (e.g., name, title, organizational division, business email and phone), and includes other information (e.g., security clearance, citizenship) that is necessary to verify the individual’s authorization to receive classified or other controlled unclassified information under the program.</p> <p>Although it is not typical or expected, PII embedded in information collected by DIB companies for cyber incident response and analysis purposes is reviewed by DC3 personnel to determine whether that PII is relevant and necessary for subsequent analysis. Information deemed irrelevant and unnecessary for subsequent analysis is purged from DC3 systems.</p> <p>Cyber incident information containing PII may be shared for law enforcement or counter intelligence purposes to support an investigation and prosecution of any individual or</p>

5. Use Limitation	Response
	<p>organization when the information appears to indicate activities that may violate laws, including those attempting to infiltrate and compromise information on a DIB company information system. Such disseminations must be approved by the Director, DC3, and comply with the Privacy Act and all other applicable statutes, regulations, and DoD policies.</p> <p>Additionally, in the section of the PIA addressing releasing PII to “Other Federal Agencies,” it states that PII is shared with other federal agency authorized personnel only for cybersecurity purposes (as authorized by the DIB companies) and following the incident response and follow-on analysis coordination procedures, and in support of authorized LE/CI activities (or other lawful purposes). Only PII that is authorized by the company will be released outside of the DoD.</p>
<p>Please describe any steps taken to mitigate any use of PII that is not specified in the applicable notices.</p>	<p>All PII is provided to DoD by a participating DIB company based on that company’s determination that the PII is relevant and necessary to incident response and analysis, and that there are no legal, contractual, or other restrictions on sharing that PII with the government.</p> <p>PII collected by DIB companies in connection with incident reporting and response is reviewed by DC3 personnel to determine whether that PII is necessary for subsequent analysis in furtherance of its DIB CS/IA Program activities. Information deemed unnecessary for subsequent analysis is purged from DC3 systems. Information determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes). The length of cyber-intrusion forensics analysis and damage assessments varies.</p>
6. Data Quality and Integrity	Response
<p>What steps are taken to ensure the continued quality and integrity of data maintained within system?</p>	<p>While the DIB CS/IA Program staff periodically review POC PII, it is incumbent upon the DIB company to provide accurate and updated POC information.</p>
<p>Please describe steps that are taken to ensure the continued confidentiality, availability, and integrity of PII</p>	<p>The System of Records is certified and accredited in order to maintain confidentiality, availability, and integrity in accordance with DoD policy.</p>

6. Data Quality and Integrity	Response
maintained within the system.	
Please describe the method for eliminating PII that is no longer needed.	<p>DIB company POC PII provided to support the DIB CS/IA Program administration and management is maintained only as long as the designated POC continues to represent the participating DIB company. When the DIB CS/IA Program office is notified that a POC was replaced, the POC information is updated and outdated PII is archived in accordance with NARA retention and disposal requirements.</p> <p>Any PII embedded in information collected by DIB companies that is deemed unnecessary for subsequent analysis is purged. Embedded PII determined to be relevant and necessary is maintained, controlled, and disposed of when no longer reasonably necessary for intrusion investigation, forensics analysis, and damage assessment activities (or other legal, audit, or operational purposes).</p>
7. Security	Response
Please describe any safeguards that are in place to ensure the continued security of data maintained within the system.	<p>The published SORN DCIO 01 states, “Records are accessed by DIB CS/IA Program office and DC3 personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have 'need to know'. Access to records requires DoD Common Access Card (CAC) and PIN. Physical access controls include security guards, identification badges, key cards, cipher locks, and combination locks.”</p> <p>In addition, the PIA states, “There are minimal risks associated with the PII collected in connection with the DoD-DIB cyber security information sharing activities under the DIB CS/IA Program. The Program’s information sharing activities implement administrative, technical, and electronic protections to ensure compliance with all applicable DoD policies and procedures regarding the collection and handling of PII and other sensitive information.”⁸³</p>
Please describe the method for securing data at rest in the system.	The PIA states, “All DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process

⁸³ See PIA at section 2g(2).

7. Security	Response
	to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems. In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory.” ⁸⁴
Please describe the method for ensuring data in transit is appropriately secured.	The PIA states, “All DoD information systems used to process and store PII (or any sensitive information) have undergone a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity, availability, and confidentiality of all sensitive information residing or transiting those systems. In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory.” ⁸⁵
Please describe the method for ensuring that access to data maintained within the system is limited to individuals with a need to know.	The SORN DCIO 01 states, “Records are accessed by DIB CS/IA Program office and DC3 personnel with security clearances who are properly screened, trained, under a signed confidentiality agreement, and determined to have need to know.”
If data from the system is sent electronically, what methods are in place to ensure appropriate safeguards apply?	All data that is sent from the system is encrypted per DoD standards. Access to the system is limited to authorized users, and all users are required to sign a Non-Disclosure Agreement before being granted access to the system.
Has PII within the system of records been categorized to reflect low, moderate, or high impact PII?	Yes, PII within the system was categorized as low impact. The Department established policy for categorizing PII in DoD CIO Memo, “DoD Guidance on Protecting PII,” August 18, 2006. ⁸⁶
What methods are in place to mitigate and address identified vulnerabilities to records maintained within the system?	The system is certified and accredited in accordance with DoD policy. DoD is required by statute to establish programs and activities to protect DoD information

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ See <http://dpcl.d.defense.gov/Portals/49/Documents/Privacy/DODGuidancePII.pdf>

7. Security	Response
	<p>and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of title 10, U.S. Code (U.S.C.),⁸⁷ requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis.⁸⁸ The program must provide continuously for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure.⁸⁹ The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations.⁹⁰ The program must provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems.⁹¹</p> <p>The Defense IA Program also must ensure compliance with federal IA requirements provided in the Federal Information Security Modernization Act of 2014 (FISMA).⁹² FISMA requires all federal agencies to provide information security protections for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.⁹³ Agencies are expressly required to develop, document, and implement programs to provide information security for information and</p>

⁸⁷ See <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap131-sec2224.pdf>.

⁸⁸ *Id.* at (a).

⁸⁹ *Id.* at (b).

⁹⁰ *Id.* at (c).

⁹¹ See <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title10/pdf/USCODE-2010-title10-subtitleA-partIV-chap131-sec2224.pdf>.

⁹² 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.*.

⁹³ *Id.* at § 3554(a)(1)(A) (formerly at § 3544(a)(1)(A)).

7. Security	Response
	information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source. ⁹⁴
Briefly describe the methodology for responding to and mitigating issues related to any potential breach of PII.	The DIB CS/IA Program office follows DoD’s breach reporting and mitigation policies and procedures in accordance with DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007. ⁹⁵
How are individuals with a need to know provided access to data maintained within the system of records?	Collection of PII in support of DIB CS/IA Program administrative management is provided by the DIB participating companies through DoD approved Public Key Infrastructure certificates. All PII is maintained on an unclassified standalone network supporting the analysis of malware in files provided by DIB partners, while a classified standalone network hosts the media provided by DIB partners for cyber intrusion damage assessment. Access is strictly controlled by DoD to personnel with a need to know and who have signed a non-disclosure agreement.

8. Auditing and Accountability	Response
What methods are in place to audit access to records maintained within the system?	The system is hosted and monitored by the Defense Information Systems Agency. As part of program oversight, audit trails and user access can be reviewed. Additionally, systems maintained at DC3 are certified and accredited by the U.S. Air Force.
Please describe any agency oversight mechanisms that apply to the system.	<p>The DIB CS/IA Program and its optional DECS component were reviewed by the DPCLD and the DoD Office of General Counsel.</p> <p>The collection, retention, and dissemination of PII by DoD intelligence or counterintelligence components is in accordance with the Attorney General Guidelines of 1982 contained in DoD 5240.1-R.⁹⁶</p> <p>All DoD information systems used to process and store PII (or any sensitive information) undergo a mandatory certification and accreditation process to verify that the system provides adequate measures to preserve the authenticity, integrity,</p>

⁹⁴ *Id.* at § 3544(b) (formerly at § 3544(b)).

⁹⁵ See DoD 5400.11-R, <http://dtic.mil/whs/directives/corres/pdf/540011r.pdf>

⁹⁶ See <http://dtic.mil/whs/directives/corres/pdf/524001r.pdf>

8. Auditing and Accountability	Response
	<p>availability, and confidentiality of all sensitive information residing or transiting those systems.⁹⁷ In addition, DC3 undergoes extensive inspection by the American Society of Crime Lab Directors to ensure that DC3 information handling procedures are reliable, valid, and repeatable in accordance with standards necessary for accreditation as a digital forensics laboratory.</p> <p>DoD Directive 5205.13E, “DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3),” directs the establishment of DC3 as an entity within the Department of the Air Force.⁹⁸ It also directs DC3 to serve as the operational focal point for the DIB CS/IA information sharing and digital forensics analysis activities performed to protect unclassified DoD information that transits or resides on unclassified DIB information systems and networks.</p> <p>Since DC3 is an Air Force entity, the Secretary of the Air Force is responsible to inspect system records at DC3.⁹⁹ To date, no privacy or civil liberties violations have been noted in any inspections of DC3.</p> <p>OMB Circular No. A-130, “Management of Federal Information Resources,” February 8, 1996, as amended, establishes managerial, procedural, and analytical guidelines for maintaining information records for individuals. One requirement is that a Privacy Act SORN be reviewed biennially to ensure it accurately describes the system of records and the data collected is accurate, relevant, timely and complete. Air Force Instruction 90-201, “The Air Force Inspection System,” governs Air Force inspection processes.¹⁰⁰</p> <p>None of the DIB CS/IA Program activities involves any DoD or government personnel performing any monitoring of a DIB company or other private networks. DIB</p>

⁹⁷ See PIA at section 2g(2).

⁹⁸ See <http://dtic.mil/whs/directives/corres/pdf/550513E.pdf>

⁹⁹ DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007, states, “during internal inspections, Component inspectors shall be alert for compliance with this Regulation and for managerial, administrative, and operational problems associated with the implementation of the Defense Privacy Program. Programs shall be reviewed as frequently as considered necessary by Components, or the Component Inspector General.”

¹⁰⁰ See http://static.e-publishing.af.mil/production/1/saf_ig/publication/afi90-201/afi90-201.pdf

8. Auditing and Accountability	Response
	<p>companies are responsible for monitoring, and any other security measures, on their own networks and for ensuring that there are no legal, contractual, or other restrictions on sharing PII or any other sensitive information with DoD. The only PII received by DoD under these activities is PII that is provided directly to DoD by authorized DIB company personnel.</p> <p>All PII is maintained with strict need to know and access controls by government and government contract personnel who have signed a nondisclosure agreement. An unclassified stand-alone network supports the analysis of malware in files provided by DIB companies, while a classified standalone network hosts information provided by DIB companies for cyber intrusion damage assessment. Data is purged when no longer needed.</p>
<p>Please describe methods that are in place to audit compliance with applicable laws and policies that pertain to the system.</p>	<p>32 C.F.R. Part 236¹⁰¹ provides authority for the DIB CS/IA Program and POC PII collections. Any change to this rule requires active participation of the DoD CIO through the DIB CS/IA Program Office, in coordination with DoD components, with interagency review and public comment. All DIB companies must agree to the requirements in Part 236 to be eligible to participate in the DIB CS/IA Program.¹⁰²</p>
<p>Please describe the methodology to ensure that only PII relevant to the system is maintained within the system.</p>	<p>The DIB CS/IA Program is structured around several key elements that are designed to ensure that risks are effectively addressed to safeguard privacy:</p> <ul style="list-style-type: none"> • All POC PII received by the DoD is provided voluntarily by authorized DIB company representatives, subject to mutually agreed upon restrictions; • The nature of the PII being intentionally collected is limited to ordinary business contact information for DIB company personnel; • Other PII embedded in collected information is submitted only if a DIB company has determined that the PII is relevant and necessary to cyber incident response and analysis activities, and that the PII is authorized to be shared with the DoD for these purposes; • All cyber incident reports submitted to DoD under the DIB CS/IA Program are

¹⁰¹ See 32 C.F.R. Part 236

¹⁰² See Final Rule 32 C.F.R. Part 236

8. Auditing and Accountability	Response
	<p>reviewed by the DIB company as well as DC3 personnel for PII. If PII is submitted and is not relevant or necessary, it is purged immediately.</p> <ul style="list-style-type: none"> • Once collected, access and use of PII is limited to authorized personnel that need to know and is otherwise lawful; • All DIB CS/IA Program and supporting personnel receiving access to the collected PII are required to undergo training and are subject to appropriate non-disclosure restrictions; and • PII is maintained for only as long as necessary for DIB CS/IA Program activities and is managed and disposed of in accordance with applicable records management requirements.
<p>Please describe any methods to ensure continued compliance with the FIPPs.</p>	<p>Continued DIB CS/IA Program compliance with DoD Directive 5400.11,¹⁰³ “DoD Privacy Program,” May 8, 2007 and DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007 will ensure FIPP compliance.</p>

¹⁰³ See <http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf>

III. CIVIL LIBERTIES ASSESSMENT

DoD's review of the DIB CS/IA Program activities found no civil liberties issues requiring discussion and assessment beyond those already identified in the privacy assessment above. The incorporation of the FIPPs into the program's activities facilitates compliance with DoD policies and procedures regarding the maintenance of PII and the protection of civil liberties.

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

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

1. Civil liberties are fundamental rights and freedoms protected by the Constitution of the United States.
2. The Department of Defense will protect the civil liberties of DoD employees, members of the Military Services, and the public to the greatest extent possible, consistent with its operational requirements.
3. The Department of Defense will consider appropriately civil liberties in the review, development, and implementation of new or existing laws, regulations, policies, and initiatives.
4. No information shall be maintained on how an individual exercises rights protected by the First Amendment to the Constitution of the United States, including the freedoms of speech, assembly, press and religion, except when:
 - Specifically authorized by statute;
 - Expressly authorized by the individual, group of individuals, or association on whom the record is maintained; or
 - The record is pertinent to and within the scope of an authorized law enforcement, intelligence collection, or counterintelligence activity.

The DIB CS/IA Program adheres to the principles and the DoD Civil Liberties Program. Multiple DoD Component offices, including the DPCLD and the DoD Office of General Counsel, were consulted with during the development of the DIB CS/IA Program to ensure that civil liberties protections were embedded in the program. These efforts incorporated the FIPPs into the DIB CS/IA Program to allow the Department to avoid activities that might violate an individual's civil liberties. The DIB CS/IA Program Office will continue to work with existing inspection agencies to certify that appropriate privacy and civil liberties oversight mechanisms are in place.

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

The DIB CS/IA Program is a cooperative cyber security program for the benefit of DoD and those DIB companies that participate in the program voluntarily. The operation of the program complies with DoD Civil Liberties Program policy. Based on the purpose, design, and function of the program, appropriate civil liberties protections are incorporated into the DIB CS/IA Program.

Recommendations

The DIB CS/IA Program, as currently structured and implemented, complies with privacy and civil liberties safeguards guaranteed by Federal law and DoD regulations, policies, and procedures. Through the ongoing collaboration of multiple DoD Components, including the Office of the Chief Information Officer, the DIB CS/IA Program Office, and the DPCLD, DoD will continue to monitor the activities of the DIB CS/IA Program as it protects our Nation's critical infrastructure from cyber threats in a manner that preserves individual privacy and civil liberties.

In Fiscal Year (FY) 2015, DoD will continue to expand industry participation in the DIB CS/IA Program. Additionally, as the Department moves toward implementation of mandatory reporting in response to Section 941 of the National Defense Authorization Act (NDAA) for FY 2013 and Section 1632 of the NDAA for FY 2015, DoD will review processes and procedures to ensure privacy and civil liberties protections continue to be effective. This includes updating applicable documentation such as the DIB CS/IA Program PIA and SORN, as necessary.

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. 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. Further, the SAOPCL must conduct assessments of their agencies’ activities and provide those assessments to the Department of Homeland Security (DHS) for consideration and inclusion in a report compiled by the DHS Privacy Office and Office for Civil Rights and Civil Liberties. In April 2014, the Department of Justice (“DOJ” or “the Department”) submitted its first privacy and civil liberties assessment for inclusion in the 2014 government-wide report.

This assessment discusses the Department’s role in implementing certain provisions of the EO and related initiatives, discussed below, during the reporting period of November 15, 2013 to September 30, 2014. During this reporting cycle, the Department participated in an interagency working group to coordinate the review and revision of the 2015 government-wide report. This working group is led by representatives from DHS and the National Security Council (NSC). Through these working group discussions and meetings, the Department has consulted with the Privacy and Civil Liberties Oversight Board (PCLOB) and has incorporated the PCLOB’s feedback on matters relating to both substance and format.

Three provisions of the Executive Order concern the Department’s cyber threat information sharing activities:

- Section 4(a) provides: “It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.”
- Section 4(b) provides: “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.”

- Section 5(a) provides: That “[a]gencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities,” and provides that “[s]uch protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.”

The Department has engaged in cybersecurity information sharing under the Executive Order related to the protection of critical infrastructure through activities undertaken by the Federal Bureau of Investigations (FBI). Thus, this report addresses the FBI’s activities in each of the sections outlined below. Section II of this assessment describes the privacy and civil liberties framework of the Department and addresses FBI’s privacy program and its internal guidance. Section III provides an overview of the FBI’s cybersecurity framework. Section IV describes the activities engaged in by the FBI under the EO and activities that, although not directly undertaken pursuant to the EO, align with its goals. Finally, Section V provides the Department’s conclusions and recommendations for future reporting cycles. The Department has also included two attachments outlining the application of the FIPPs in chart format to the two activities, which align with the goals of the Executive Order.

II. Department’s Privacy and Civil Liberties Framework

Cyber intrusions into critical infrastructure pose a serious threat to our national security. Under EO 13636, agencies are to enhance their sharing of information related to cyber threats with U.S. private sector industries. Information sharing, however, can carry risks to the privacy and civil liberties of individuals. Thus, EO 13636 also requires agencies to evaluate their cybersecurity information sharing activities against the FIPPs and other privacy and civil liberties policies, principles, and frameworks. This section discusses DOJ’s Department-wide privacy program, including its privacy compliance process, which identifies and mitigates privacy risks during the development and implementation of Department systems or programs. This section also discusses FBI’s internal privacy program, and the guidelines and principles governing the FBI’s operations.

A. Department-wide Privacy and Civil Liberties Protections

The Department established the position of the Chief Privacy and Civil Liberties Officer (CPCLO) within the Office of the Deputy Attorney General (ODAG), and created the Office of Privacy and Civil Liberties (OPCL) to oversee the Department’s privacy compliance process and to ensure that appropriate privacy and civil liberties protections are incorporated into the Department’s systems, programs, and operations, including those that involve cybersecurity. The CPCLO’s statutory responsibilities include advising the Attorney General regarding: appropriate privacy protections relating to the collection, storage, use, disclosure, and security of personally identifiable information (PII) with regard to the Department’s existing or proposed information systems; the implementation of policies and procedures, including appropriate training and auditing, to ensure the Department’s compliance with privacy-related laws and policies; and privacy-related reports from the Department to Congress and the President.¹ In addition, the Department has established within each of its

¹ Section 1174 of the Violence Against Women and Department of Justice Reauthorization Act of 2005 required the Attorney General to designate a senior official in the Department of Justice to assume primary responsibility for privacy policy.

components a Senior Component Official for Privacy (SCOP) to be accountable for their component's privacy program.

The Department protects privacy and civil liberties in a variety of ways. One main way is through the Department's privacy compliance process, which begins with the Initial Privacy Assessment (IPA). The IPA is a tool designed to assist Department components with identifying privacy issues during the development of an information system in order to help resolve and mitigate any such concerns, and to assist Department components in determining whether additional privacy documentation is required by either the Privacy Act of 1974² (e.g., a System of Records Notice (SORN)) or Section 208 of the E-Government Act of 2002³ (e.g., a Privacy Impact Assessment (PIA)). The use of IPAs in the privacy compliance process ensures that an opportunity exists to examine all new or modified information systems and programs for potential privacy and civil liberties concerns. PIAs, required by Section 208 of the E-Government Act of 2002, address the existing authorities permitting the collection and advanced analysis of information.⁴ As with the IPA, PIAs are an integral part of the Department's privacy compliance process and have been incorporated into the Department's IT security framework, which ensures that all IT systems that require PIAs are identified and allows the Department to resolve or mitigate privacy risks they may pose. Moreover, the Department has long been subject to the Privacy Act of 1974. Through the privacy compliance process, components work internally and with OPCL to review and resolve Privacy Act issues as they arise. Finally, the CPCLO and OPCL are asked to review various privacy and civil liberties issues impacting the Department's programs and operations.

B. FBI's Privacy and Civil Liberties Protections

As part of the Department's privacy and civil liberties framework, each component also reviews and implements privacy and civil liberties policies and requirements. As stated above, each component has designated a SCOP to be accountable for its privacy program. The FBI has had a long-established Privacy and Civil Liberties Officer (PCLO). This PCLO, who is also a Deputy General Counsel, has been designated as the FBI SCOP. The FBI's SCOP is supported by a Privacy and Civil Liberties Unit (PCLU) in the Office of the General Counsel (OGC), which provides legal and policy guidance within the FBI related to privacy and civil liberties issues, including those that affect cybersecurity issues. The FBI's OGC Cyber Law Unit provides additional legal support regarding cyber matters, and the Department's CPCLO and OPCL also work closely with FBI. It is through this structured approach leveraging subject matter expertise that the Department can identify and address privacy and civil liberties issues systemically, while providing the unique attention to detail associated with each discrete question, including those that relate to cybersecurity information sharing.

In addition to the laws and framework described above, the FBI adheres to the Constitution, Executive Order 12333, and other relevant guidance, such as the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), and internal operational guidelines, such as the FBI Domestic Investigations and Operations Guide (DIOG).⁵ In particular, Section 4 of the DIOG

² 5 U.S.C. § 552a (2012).

³ See 44 U.S.C. § 3501 (note) (2012).

⁴ *Id.*

⁵ The FBI adheres to the protection of civil liberties in all of its activities. As set forth in the AGG-DOM, Section I.C.3, "[a]ll activities under [the AGG-DOM] must have a valid purpose consistent with these [AGG-DOM], and must be

(Privacy and Civil Liberties, and Least Intrusive Methods) provides substantial guidance to FBI personnel to ensure FBI activities protect the public's privacy and civil liberties.⁶ Moreover, the Attorney General has provided federal law enforcement officers with updated civil rights guidance for conducting law enforcement activities. This guidance stipulates that law enforcement officers may only consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity to the extent that trustworthy information relevant to the locality or time frame links persons possessing a particular listed characteristic to an identified criminal incident, scheme, organization, threat to national or homeland security, violation of federal immigration law, or authorized intelligence activity. The FBI is bound by the DOJ Use of Race Policy by Federal Law Enforcement Agencies, which extends civil liberties protections to law enforcement activities undertaken by federal law enforcement, including those related to national security. The DIOG, Section 4.3.1, imposes these requirements, as well.⁷ Race, ethnicity, religion, or national origin alone can never constitute the sole basis for initiating investigative activity.⁸ Although these characteristics may be taken into account under certain circumstances, there must be an independent authorized law enforcement or national security purpose for initiating investigative activity. Thus, the requirement to protect Americans' civil liberties is an important aspect of all FBI investigative activities, including cyber investigations.⁹

III. Overview of the Department's Cybersecurity Framework

DOJ investigates, attributes, and disrupts cyber threats to the United States by enforcing federal laws and by collecting and disseminating intelligence using integrated law enforcement and national security authorities. Specifically, these cyber threats involve computer intrusions and attacks conducted by criminal and national security threat actors that impair the confidentiality, integrity, or availability of a computer, device, or data, or are likely to result in the compromise or loss of sensitive personal data, proprietary commercial data, or sensitive or classified government information.¹⁰

The FBI has primary responsibility for investigating violations of federal law and for collecting foreign intelligence and counterintelligence in the United States, and accordingly, plays a critical role in protecting cybersecurity. Section 2.2.1 of the DIOG authorizes the FBI 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. Specifically, the FBI has authority to investigate computer fraud and intrusion violations under 18 U.S.C. §1030, and has primary authority to investigate such offenses involving espionage, foreign counterintelligence, and information protected against unauthorized disclosure for reasons related to the national defense or foreign relations or restricted data, except for those offenses statutorily

carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines.

⁶ See FBI DIOG (October 15, 2011) (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/).

⁷ *Id.*

⁸ *Id.*

⁹ 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.

¹⁰ U.S. Dept. of Justice, Cyber Threat Strategic Report (May 16, 2014), at 5.

assigned to the United States Secret Service. In fulfilling its mission to defeat malicious cyber adversaries, the FBI recognizes the need to enhance information sharing with the private and government sectors to defend against these varied threats, as evidenced by the cyber initiatives delineated below.

The FBI's Cyber Division (CyD), facilitated by its 24-hour cyber command center (CyWatch), has merged its investigative and intelligence capabilities to combat cyber threats and to maximize the government's ability to identify, pursue, and defeat cyber adversaries targeting global U.S. interests. Through the National Cyber Investigative Joint Task Force (NCIJTF), led by the FBI, federal agencies are able to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force to pursue the malicious actors behind cyber attacks. After the implementation of Next Generation (Next Gen) Cyber,¹¹ the CyD was tasked with managing investigations into computer intrusions targeting national information infrastructure, Internet-facilitated criminal activity, and supporting other major divisions with cyber matters.¹²

As part of its cybersecurity investigative process, the FBI shares cyber threat information, as appropriate, with both its U.S. government partners and with the private sector. For example, this information can help the FBI and the intelligence community (IC) understand the actions, goals, methods, and capabilities of those posing threats, and to anticipate and prevent future attacks against the private sector, critical infrastructure, and government systems. Recognizing that cyber threats to both government and private systems can affect our national security, the FBI also provides the private sector with in-person cyber threat classified and unclassified briefings so that they may understand the current threats and assist law enforcement's efforts in protecting critical infrastructure.¹³ The Cyber Initiatives and Resource Fusion Unit, which is co-located with the National Cyber Forensics and Training Alliance (NCFTA), is a coalition between industry subject-matter experts and law enforcement to collaborate on initiatives targeting cyber crime. At NCFTA, law enforcement members work side-by-side with representatives from the private sector to address significant cyber threats and exchange strategic intelligence.

The EO is a critical framework for improving information sharing with the private sector; however, it does not encompass all of the FBI's critical infrastructure information sharing activities. There are

¹¹ Next Gen Cyber was an initiative to strengthen the FBI's ability to combat cyber threats and adapt to rapidly evolving technology. The initiative consisted of two key shifts for FBI CyD: (1) focusing CyD's efforts on intrusions, in which adversaries break into computers to steal information or to disrupt infrastructure; and (2) enhancing the technological capabilities of all FBI personnel.

¹² Many of these initiatives predated the issuance of EO 13636.

¹³ FBI CyD shares cyber threat information with U.S. private sector entities through various methods. This information sharing aligns with the goals of the EO. The National Cyber Investigative Joint Task Force (NCIJTF) and CyWatch provide rapid dissemination of unclassified information through tools known as the FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs), although these types of reporting do not identify specific targeted entities. FLASH reports contain critical technical information collected by the FBI for use by specific private sector partners, and are intended to provide recipients with actionable intelligence that will aid in timely victim notification and response. Similarly, PINs contain current information that will enhance the private sector's awareness of a threat. Analysts are encouraged to produce a PIN when information is collected that indicates a potential harm to, or addresses equities in, the private sector. PINs may be re-formatted into formal FBI intelligence products. To ensure that privacy and civil liberties protections are taken into account in the PINs and FLASH process, CyWatch is required to adhere to the FBI DIOG, which includes sections regarding information dissemination, as well as incorporates Privacy Act requirements and civil liberties protections for collection, maintenance, and dissemination of information.

several activities conducted by the FBI related to such information sharing that may not be within the scope of the EO, such as the FBI's engagement with the private sector through the Bureau's 56 field offices, as well as FBI Headquarters' numerous outreach programs, including the CyD's Cyber Operations and Outreach Section, FBI's InfraGard program,¹⁴ the Domestic Security Alliance Council (DSAC),¹⁵ and its CyD and National Cyber Investigative Joint Task Force (NCIJTF). As such, these activities will not be discussed in detail in this report.

The FBI has a robust cyber threat information sharing program, and those activities are conducted while protecting individual privacy and civil liberties. The FBI does encourage victims to share as much threat information as possible, with both the private sector and the government, to mitigate the effects of the crime and assist law enforcement efforts to bring the perpetrators to justice, but the FBI does not compile records regarding the interactions between private enterprises victimized by cyber intrusions and their customers. Information associated with cyber threats is often technical, and rarely involves PII. However, if PII were relevant to the cyber threat, FBI would share such information to meet its mission needs in combating malicious cyber activity in accordance with the authorities and protections described above.

In addition, if PII obtained for cybersecurity purposes became relevant to another type of investigative purpose such as fraud, that information could only be shared consistent with FBI legal authorities. Even within a permissive sharing context, the FBI carefully scopes information in order to minimize risks to privacy and civil liberties as a matter of general practice. An example of risk minimization would include manual review, limited access to information, or supervisory approval. Furthermore, the FBI will continue to develop policies and procedures for information sharing and privacy and civil liberties protections as these initiatives mature.

¹⁴ InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

¹⁵ DSAC is a strategic partnership between the U.S. Government and U.S. private industry. Its goal is to increase security by enhancing communications and promoting the timely and effective exchange of security information among its constituents. DSAC advances the FBI's mission of preventing, detecting, and deterring criminal acts by facilitating strong, enduring relationships among its private industry members, FBI Headquarters divisions, FBI field offices, DHS Headquarters, DHS Fusion Centers, and other Federal Government entities. DSAC also advances the U.S. private industry's ability to protect its employees, assets, and information by providing ongoing access to security information and to a network of security experts, and by providing continuing education for corporate chief security officers and intelligence analysts.

IV. Cyber Information Sharing Activities

This report discusses cyber information sharing activities conducted by the Department during the period from November 15, 2013 to September 30, 2014. Specifically, the report references the Department's issuance of the ODAG order last year to implement Section 4(a) of the EO, and its implementation of Section 4(b) of the EO, which includes the activities concerning interagency discussions to develop a process to address the 4(b) requirements. This report also discusses two FBI initiatives that, if fully implemented, are intended to promote the sharing of cyber threat information with the private sector, namely the iGuardian initiative and Malware Investigator.

A. Implementation of Section 4(a)

This privacy and civil liberties assessment focuses primarily on Section 4(b) of the EO, but for context of the report, it is worthwhile to note the prior activity of Section 4(a). Section 4(a) of the EO provides: "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of Section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations."

In last year's assessment, the Department of Justice noted that in accordance with Section 4(a), 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.¹⁶ The Order also requires that all actions taken pursuant to the Order must be consistent with the need to protect privacy and civil liberties. During the current reporting cycle, there are no further updates regarding the implementations of Section 4(a).

B. Implementation of Section 4(b)

Section 4(b) provides: "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." To implement Section 4(b), FBI, DHS, the Department of Defense (DOD), and the Office of the Director of National Intelligence (ODNI) conducted a pilot using FBI's Guardian system to collect information on cyber incidents, and after

¹⁶ U.S. Dept. of Justice, Order 3393, Issuing Instructions Pursuant to Executive Order 13636 Regarding the Timely Production of Unclassified Reports of Cyber Threat Information (2013).

the pilot established an interagency working group to address the requirements needed to develop a new 4(b) system. In addition, the FBI has provided information on its iGuardian initiative and Malware Investigator, which are activities that, although not undertaken specifically pursuant to EO 13636, align with the goals of the Executive Order to improve information sharing of cyber threats between the United States government and the private sector. These activities are discussed below.

1. Pilot of Guardian Cyber

Immediately following the issuance of the EO in February 2013, the FBI, DHS, DOD, and ODNI developed a process to meet the requirement in Section 4(b) for providing a system to track the production, dissemination, and disposition of cyber threat reports to specific targeted private sector entities. In 2013, DHS and FBI discussed the use of piloting the use of Guardian for Cyber (Guardian Cyber) on SIPRNET¹⁷ as a potential system to track the production, and dissemination of cyber threat reports to specific targeted private sector critical infrastructure entities.

In order to facilitate 4(b) sharing, the FBI and DHS entered into a memorandum of agreement relating to the use of the Guardian Cyber pilot. During the pilot, DHS users were required to abide to the same rules as FBI employees for purposes of accessing Guardian. The pilot program demonstrated, however, that the requirements needed for an interagency system varied from the requirements that had been developed for the Guardian system for use by the FBI for tracking and assessing terrorism suspicious activity reports. Thus, FBI and DHS have placed the actual sharing of information through this pilot on a temporary hold, pending further development of policy issues related to the requirements for the 4(b) system.

2. Joint Requirements Team

With guidance from NSC staff, FBI, DHS, and DOD developed an interagency Joint Requirements Team (JRT) to develop requirements for a system that meets the Section 4(b) mandate. The JRT recognizes that while the Section 4(b) mandate could be accomplished through modifications to the Guardian platform, additional business processes, including a governance structure, will need to be developed to support implementation of the concepts. As these business processes are developed, the JRT will work with each agency's privacy subject matter experts (SMEs) to ensure that privacy and civil liberties protections are built into the process, in accordance with the FIPPs and Section 5 of the EO. The goal of the JRT is to fully mature the interagency process and to share cyber threat information with specific targeted entities (sometimes referred to as "victim notification").

The progress of the JRT and the development of the 4(b) solution may be discussed in next year's EO 13636 privacy report. Also, if a system were developed that met the requirements of a system of records under the Privacy Act, the public would be notified of its creation through the issuance of a SORN. To date, however, there has been no determination as to the precise structure of a 4(b) system. Therefore, it would be premature to discuss which, if any, agency would be issuing a SORN. The specific privacy and civil liberties protections that governed the pilot program were the same that govern the Guardian system. In particular, the privacy risks were mitigated by protocols that include access controls, auditing, and credentialing. In addition, the standard for sharing PII

¹⁷ 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.

will be one of the considerations of the JRT as it develops the business processes for interagency sharing of cyber threat information.

C. FBI's Cyber Activities that Align with EO 13636

1. iGuardian

iGuardian is a template submitted voluntarily via a web portal regarding cyber intrusion complaints from the private sector and from certain law enforcement (LE) entities. The FBI initially developed and piloted iGuardian as a means to receive information from the private sector; however, as iGuardian has evolved it may not technically fall within the scope of the EO. However, the FBI's use of iGuardian aligns with the goals of the EO—enhanced sharing of cyber threats between the private sector and the government, and if iGuardian is further developed, it may play a more significant role in the FBI's implementation of the EO. In the interest of transparency, the Department and the FBI, in consultation with representatives from the PCLOB, have assessed the privacy and civil liberties protections for this activity, which is included as Attachment A.

Currently, a particular entity's method for submitting cyber incidents to iGuardian depends on whether it is a private sector entity or a law enforcement entity. As described in the Department's 2013 assessment, the private sector entities that will submit cyber intrusion complaints to the FBI through iGuardian will be members of InfraGard, a public-private partnership between the FBI and members of the private sector who are focused on intrusions and vulnerabilities affecting the critical infrastructure sectors. Any private sector entity wishing to submit a suspicious cyber report to the FBI through iGuardian must first submit an application to the FBI to become a trusted InfraGard partner. Once the FBI has vetted the application and determined that the entity is a trusted partner, the user will be able to log into iGuardian through the InfraGard website.¹⁸ An additional and notable development that occurred during this reporting period is that the FBI opened iGuardian up to vetted state and local enforcement entities through the Internet Crime Complaint Center (IC3) in order to maximize threat reporting.

Once a user has accessed iGuardian, the user is able to complete an online incident reporting form, attach relevant files, and transmit relevant cyber threat information to the FBI. A completed form may include the following items of information:

- (a) Submitter's contact information (such as name, phone number, and email address);
- (b) Information about submitter's organization (such as name and address);
- (c) 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);
- (d) Information regarding the threat's target or objective (such as the incident sector, the incident type, and the IP address of the target); and

¹⁸ In the future, the FBI plans to allow InfraGard members to access iGuardian through the iLaw Enforcement Enterprise Portal (iLEEP)—a secure website that will allow the FBI's entire network of trusted private sector partners to share information with the FBI using a single authentication. Currently, a few companies are participating in a pilot program in which they are able to access iGuardian through LEEP, a secure website that ordinarily provides law enforcement entities with access to FBI systems using a single authentication; once iLEEP is operational, these companies will transition from LEEP to iLEEP.

- (e) Information regarding damage/impact to submitter's organization.

For users who are cleared defense contractors or who represent cleared defense facilities, a completed form may include the additional items of information:

- (a) Information regarding submitter and submitter's organization (such as title, location, and commercial and government entity code);
- (b) Contract information, including names of points of contact;
- (c) Information regarding targeted technology, program, or contract;
- (d) Information regarding the system's role, function, and location; or
- (e) Whether the affected information is export-controlled or classified.

The type of information provided on the iGuardian Incident Submission concerns the type of cyber incident being reported by the company, including technical details regarding the incident. Other than information concerning the employee submitting the information, no specific PII about employees is requested. Submitters may provide additional details about the incident. iGuardian itself does not store any of the information provided in the complaints. Rather, once it is transmitted by a user, the information is routed through the iGuardian system to the Guardian Cyber system, where each submission resides and receives individualized review.¹⁹ At this time, the FBI is not considering automated review of intrusion complaints until further utility of the system is determined.

2. Malware Investigator System

Malware Investigator is an FBI initiative developed in collaboration with federal, state, and local law enforcement, the intelligence community, and private sector partners to encourage sharing of technical data about malware functionality, analytical tools, standards for sharing metadata and threat scoring, and develop technical solutions for automated exchanges. Malware Investigator is hosted by the FBI's Law Enforcement Enterprise Portal (LEEP), which is covered by separate privacy documentation.²⁰ The FBI began developing and using Malware Investigator prior to the issuance of the EO by sharing technical data. It is important to note that sharing technical data is different than providing cyber threat reports. Malware Investigator works by primarily receiving malware²¹ from the private sector. However, the FBI's use of the system aligns with the EO, and when the system is more fully developed, it may play a more significant role in the FBI's implementation of the EO. For this reason, and in the interest of transparency, the Department and

¹⁹ iGuardian submissions are fed into FBI's Guardian Cyber system through eGuardian. Submissions into iGuardian are at the unclassified level, which enables private sector entities to transmit threat reports to the FBI. Guardian Cyber is a classified system (collateral SECRET), which resides on SIPRNET. Guardian Cyber was developed from the Guardian system, which was developed initially by the FBI to collect suspicious activity regarding terrorist threats and to triage, assign, and assess such information. iGuardian data from private sector submissions transits through Guardian Cyber via eGuardian but is not analyzed, stored, or handled by the FBI in eGuardian; after it is assessed, it resides in Guardian Cyber. As described in Attachment A, a PIA was conducted on the Guardian system, but as a national security system, the PIA is not publicly available.

²⁰ The FBI's Law Enforcement Enterprise Portal (LEEP) is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources. One LEEP service is N-DEx. The N-DEx PIA is available at <http://www.fbi.gov/foia/privacy-impact-assessments/N-DEx>.

²¹ Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.

the FBI, in consultation with representatives from the PCLOB, assessed the privacy and civil liberties of this activity, which is included as Attachment B.

Malware Investigator provides trusted FBI partners with an unclassified, automated malware analysis system that analyzes suspected malware and quickly returns technical information to users so that they may understand the functionality of the malware submitted. It also allows users to correlate malware samples and collaborate with others. Providing this solution will enable the FBI to offer services to these entities while also assisting the intelligence and law enforcement communities in developing an accurate threat assessment. Thus, this system will fulfill the need for a consolidated malware repository, as it provides a global perspective of malware threats, and will provide for advanced technical analysis and collaboration among the federal government and its partners.

To access Malware Investigator, most users login through the LEEP portal to submit suspicious files to the FBI. The results users receive back consist of an analysis of those files. There will also be application programming interface (API) access allowed by entities authorized by FBI to have access through an API.²² API allows machine-to-machine communication without user interaction. Currently, only LE entities have access to Malware Investigator. However, in the future, the FBI plans to permit private sector partners to submit suspicious files to the FBI through Malware Investigator. In most cases, LE submissions are submissions of suspicious files acquired lawfully from state and local public and private sector victims. Private sector partner submissions may be provided directly from the private sector victims. In some cases, LE submissions are on behalf of the LE entity's own federal, state, or local LE agency, and thus, the LE entity submitting the information is the victim. As mentioned above, civil liberties are the bedrock foundation of all the information that the FBI collects.

V. Recommendations to Enhance Privacy and Civil Liberties Protections

A. iGuardian Recommendations

With respect to iGuardian, the FBI will review whether private sector entities would benefit from training, including instruction on marking information that may be considered proprietary, or require further restrictions on dissemination so that the FBI may easily recognize such information and treat it in accordance with any restrictions. Additionally, the FBI will work with the iGuardian program management to provide notice to authorized iGuardian users that they must determine their own authority to submit information to the FBI. If the submission contains PII regarding their employees or others, the iGuardian user must determine whether it is authorized to provide the information and whether it is relevant to the submission. The FBI should also work with stakeholders and the private sector to determine appropriate levels of training and outreach. The FBI should review whether it provides adequate information to allow the public to understand why the FBI has established iGuardian, and how the information collected will be used to combat cyber threats.

Relating to information sharing, iGuardian incidents are currently reviewed by an FBI Cyber Watch investigator to determine if the incident warrants additional action. If the incident warrants additional action because it is deemed to be a credible complaint, it is assigned to the appropriate

²² Authorized NCFITA users may access Malware Investigator through an API.

FBI entity for further review and investigation. At this stage in the iGuardian lifecycle, only relevant information is transferred to Guardian Cyber. Information determined to be relevant is reviewed by trained Cyber Watch specialists for further review. Should iGuardian continue to be used, the FBI will continue to examine information sharing procedures and policies to ensure it shares information with the private sector to the full extent permissible by law, while protecting the privacy and civil liberties of individuals.

The FBI will enhance privacy and civil liberties protections and address potential risks for iGuardian Incident Submissions as this initiative matures. Even though limited PII is collected on the iGuardian Incident Submission form and information is submitted by the corporate victim on a voluntary basis, as the system and user base develop, enhanced privacy and civil liberties protections will be needed. As appropriate, the FBI will address increased transparency, data security, integrity and access, accountability, and training. Although members of the general public will not be users of the system, the private sector companies and their individual representatives vetted as InfraGard members that submit information through iGuardian may benefit from increased transparency. As a result, the public should be apprised of the purpose of iGuardian and how an individual's electronic interaction with a company may or may not be used in the course of reporting a cyber incident.

B. Malware Recommendations

The recommendations to enhance privacy and civil liberties protections for Malware Investigator are similar to those for iGuardian. Generally, the FBI's recommendation for Malware Investigator is to audit the submissions from law enforcement and determine whether any PII was submitted. Currently, Malware Investigator is only open to LE and IC personnel. As a valuable tool for sharing cyber information, the public, as well as state, local, and private sector entities, may benefit from learning more about the system. Accordingly, CyD will examine ways in which to increase transparency and better inform the public about the purpose of the system and the limited information collected. Although the private sector does not currently use the system, law enforcement may submit information on the behalf of victims, and thus the victims may want additional information about how Malware Investigator collects, maintains, and disseminates their information. As it relates to Malware, when the FBI opens Malware Investigator to private sector partners, the FBI will undertake a review of the system to ensure that only technical information is provided and that any inadvertently submitted PII is minimized and not further used. In future reports, the FBI will examine the ways in which information submitted to Malware Investigator was useful in assisting victims.

Similar to the second recommendation for iGuardian, the FBI will examine whether additional outreach is needed to ensure that information submitted to Malware Investigator by law enforcement is for the purpose specified. As described above, the system's design permits very little deviation from the intended purpose, but the FBI will continue to assess this system to ensure that the information submitted relates to potential malicious code. Further, the FBI should examine whether LE entities need increased training or additional instruction on marking information that may be considered proprietary, or require further restrictions on dissemination in order for FBI to more easily recognize such information and treat it accordingly. As mentioned above, the FBI will continue to review and revise its internal information sharing policies, as necessary.

C. Conclusion

Overall, the FBI CyD's privacy and civil liberties framework for private sector information sharing of cybersecurity threats continues to provide a multi-layered approach to the incorporation of the FIPPs, as well as other privacy and civil liberties protections through oversight and advice, including the development of formal policies and training, as well as through IPAs, PIAs, and the SORN process. The Department will assess any civil liberties issues as they may arise going forward with the FBI's activities under the EO, such as ensuring that the same protections required to be followed by the FBI are used as "best practices" for any interagency system developed to implement Section 4(b) of the EO. The Department will continue to conduct its investigative, prosecutorial, and intelligence responsibilities consistent with the laws and policies that protect privacy and civil liberties. The protection of privacy and civil liberties is at the forefront of all of CyD's activities as it implements the EO to inform specific targeted entities of the current cyber threat landscape facing them, not only today, but in the future.

Attachment A

In accordance with Section 5(b) of the EO, this assessment includes an evaluation of activities that align with the EO (although not undertaken pursuant to 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 PII by the FBI's CyD when sharing and receiving information with the private sector for the purpose of protecting the cybersecurity of critical infrastructure.

In addition to the FIPPs, the Department considers other applicable privacy and civil liberties policies, principles, and frameworks. For example, this chart includes information on how FBI adheres to federal privacy laws such as the Privacy Act and Section 208 of the E-Government Act. As noted above, iGuardian may not fall within the scope of the EO. However, the FBI's use of iGuardian aligns with the goals of the EO, and if iGuardian is further developed, it may play a more significant role in the FBI's implementation of the EO. The Department has no indication of any activity warranting a civil liberties review. At this time, iGuardian and Malware Investigator are new systems and will be continuously reviewed for privacy and civil protections as these initiatives develop. The Department will evaluate the manner in which to assess civil liberties issues with respect to cyber information sharing activities under the EO going forward, including by reviewing the efforts of the JRT and future developments of iGuardian and Malware Investigator.

iGuardian FIPPs Chart

(a) Transparency
<p>1. How does the FBI incorporate the principle of transparency into iGuardian?</p> <p>Response: For Privacy Act purposes, iGuardian login information is covered under Privacy Act SORN, DOJ-002, DOJ Computer Systems Activity and Access Records.²³ Although iGuardian itself does not store any of the information provided in the complaint, once the complaint is transmitted by a user, the information is routed through the eGuardian system to the Guardian Cyber system, where each submission resides and receives individualized review.²⁴ Any information ultimately maintained by FBI, would be covered by 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). Additionally, the FBI has published a PIA on eGuardian. http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat. Guardian is also noticed under Privacy Act SORN, FBI-022, Data Warehouse System. Because Guardian is national security system, the PIA is not publicly posted. Constructive notice of these systems is provided by the applicable SORNs.</p> <p>When a private sector partner applies for iGuardian access by being vetted as an InfraGard member, the partner is 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 InfraGard does not provide express notice regarding the treatment of third party information, InfraGard members must agree to the membership responsibilities and bylaws that require good faith submission of accurate information. Each iGuardian user’s first and last name, telephone number, email address, job position, company name, company industry sector, and company address, are collected on the application form. In addition, the form also requires the user’s first and last name, telephone number, email address, and job position or the applicant’s supervisor or Chief Security Officer for validation purposes.</p> <p>Furthermore, all InfraGard members must agree to bylaws that include a statement of ethics. This ethical code requires participants to conduct themselves in compliance with all applicable federal, state, and local laws. For example, InfraGard participants must not engage in illegal activity by knowingly submitting false or misleading information to InfraGard. InfraGard is committed to establishing an atmosphere of trust among its members, and this ethical code of conduct promotes better data quality and integrity.</p> <p>In addition to account information, voluntary users of iGuardian submit cyber threat information. This information may include PII about the cyber threat actor. Third party direct consent of the</p>

²³ DOJ-002, the DOJ Computer Systems Activity and Access Records SORN, available at: <http://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf>.

²⁴ iGuardian submissions are fed into FBI’s Guardian Cyber system, through eGuardian. Submissions into iGuardian are at the unclassified level, which enables private sector entities to transmit threat reports to the FBI. Guardian for Cyber is a classified system (collateral SECRET), which resides on SIPRNET. Guardian Cyber was developed from the Guardian system, which was developed initially by the FBI to collect suspicious activity regarding terrorist threats and to triage, assign, and assess such information. iGuardian data from private sector submissions transits through Guardian Cyber via eGuardian but is not analyzed, stored, or handled by the FBI in eGuardian; after it is assessed, it resides in Guardian Cyber.

<p>cyber threat actor is not practicable due to the need to protect the confidentiality of the law enforcement investigation. To the extent that a company is submitting information about its system, the company must determine that it is authorized to make that submission. As discussed above, the FBI may notify the submitters of this obligation and that any PII submitted must be authorized, relevant, and necessary to the submission. This obligation resides with the submitters to ensure they are authorized to provide information, including relevant and necessary PII, on the iGuardian submission form. In addition to allowing submitters to send a cyber threat-related file, iGuardian permits the user to enter threat information, which may include the threat actor’s name.</p>
<p>2. How does CyD ensure that issues surrounding transparency are re-evaluated on a periodic basis?</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 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 iGuardian provides sufficient transparency.</p>
<p>(b) Individual Participation</p>
<p>3. Are victims asked for consent and given the opportunity to object to the collection of their PII?</p>
<p>Response: In most cases, private sector partners will be reporting incidents or threats pertaining to their organization; and thus, the submitter or iGuardian user is the victim, and therefore will be providing consent. When iGuardian users submit incident reports, those users are required to obtain consent. All information that is submitted into an FBI database has to be consistent with civil liberties policies, including prohibitions against collecting information solely on the basis of race.</p> <p>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 private sector entity.</p>
<p>4. How does iGuardian ensure that the FBI CyD’s Victim Notification Process is implemented?</p>
<p>Response: In most cases, the private sector entity will already be aware of its status as a victim, because the entity has taken proactive steps through the use of iGuardian to notify the FBI of the incident. However, the FBI will still need to develop steps or utilize 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.</p>
<p>5. Are iGuardian users given the opportunity to access and correct their PII?</p>
<p>Response: Yes. Users may access and correct their user account information through the LEEP portal management tool and iLEEP in the future. At this time, third parties must work directly with the InfraGard submitter.</p>
<p>6. Are victims given the opportunity to access and correct their PII?</p>
<p>Response: In most cases, the private sector partners are the victims, and thus, as described above, will have the opportunity to access and correct PII. However, because iGuardian is a one-</p>

<p>way system, users will not have the ability to access specific entries of cyber threat information once the submission is transmitted from iGuardian to Guardian. If users would like to update their submissions, users are required to make a new submission or contact the iGuardian program.</p>
<p>7. Describe the mechanism provided for an individual 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 LEEP (and iLEEP in the future) at the number listed on the login page, or by contacting the iGuardian program office.</p>
<p>8. Describe the mechanism provided for a victim to seek redress in the event of inappropriate access, to or disclosure of their PII.</p>
<p>Response: Although iGuardian collects very limited PII (e.g., IP addresses), victim information, in addition to the mechanisms listed above, is covered by 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>9. What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete?</p>
<p>Response: Because the information submitted through iGuardian will, in most cases, reflect first party submissions directly from the victim, there is a diminished risk that the first party information submitted will be inaccurate, untimely, irrelevant, or incomplete. The FBI will protect third party information in the same way that protects first party information. However, once the information is submitted, as stated above, the information is transmitted through eGuardian to Guardian Cyber, where these factors will be evaluated as part of the case management process in Sentinel, as described in the PIA.²⁵ iGuardian incidents are reviewed in coordination with federal agencies with cyber security missions and by a FBI Cyber Watch 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. Guardian is a national security system. Generally speaking, Guardian has robust security mechanisms, audit capabilities, and strict user access. FBI personnel are required to complete privacy and civil liberties training before gaining access to FBI information systems.</p>
<p>10. 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, iGuardian account information and submissions of cyber threat information are collected directly from the private sector partner. There may be cases where the private sector partner submits information about the particular threat actor, and thus the submission may contain third party PII. As explained above, the information submitted is transmitted through eGuardian and then to Guardian, where these factors will be evaluated as part of the case management process described in the Guardian PIA to ensure that the information submitted is accurate and complete.</p>

²⁵ Sentinel is the FBI's system for centrally managing case file information. The PIA can be located at: <http://www.fbi.gov/foia/privacy-impact-assessments/sentinel>.

(c) Purpose Specification

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

Response: The specific purpose for the maintenance of user information is to facilitate information sharing from the private sector entity to the FBI by permitting access to iGuardian. The PII collected is limited to the information needed to vet the individual for account access and to establish an iGuardian account.

To the extent and in the unlikely situation that other information is provided, 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 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."²⁶ 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 DIOG Part II.²⁷

As a practical matter, the information submitted on the iGuardian 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.

With regard to certain uses of information that are submitted on the iGuardian incident form, such information is covered by Privacy Act SORN, FBI-002,²⁸ which describes the appropriate routine uses that may apply to information gathered through iGuardian. The information that may be collected through the portal includes names of individuals associated with the complaint, IP addresses, and other information provided by the complainant in the comments form or uploaded as an attachment.

Currently, FBI's iGuardian 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.

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

²⁶ AGG-DOM, Introduction A.

²⁷ See FBI DIOG, *supra* note 6.

²⁸ The Central Records System SORN, FBI-002, can be located at: <http://www.gpo.gov/fdsys/pkg/FR-1998-02-20/pdf/98-4206.pdf>.

Response: For initial reporting, the FBI depends on the private sector partner, who is in most cases the victim, to ensure the collection of information submitted to the FBI is validly collected. Because the partner is usually submitting information about cyber threats to its own networks and infrastructure, the risk of unauthorized collection is low. However, 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

13. Describe steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.

Response: As described above, iGuardian only permits users to perform limited functions, which consist of logging into the system, submitting cyber threat-related files, and providing an incident description. Information is submitted through a one-way transfer from the private sector partner to the FBI. Once the information is transferred to Guardian and reviewed by the FBI, 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. As previously indicated in subsection 3 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.

(e) Data Quality and Integrity

14. What steps are taken to ensure that data is accurate, timely, relevant, and complete?

Response: As stated above, iGuardian collects a limited amount of PII. When a private sector partner applies for iGuardian access, the partner is provided with a comprehensive Privacy Act Statement and other detailed information, including information about monitoring and auditing of the system for security purposes. Each iGuardian user’s first and last name, telephone number, email address, job position, company name, company industry sector, and company address, is collected on the application form. In addition, the form also requires the first and last name, telephone number, email address, and job position, or the applicant’s supervisor or Chief Security Officer for validation purposes.

For cyber threat information submitted by users to iGuardian, the likelihood that the information will be inaccurate, untimely, irrelevant, or incomplete is relatively low. Much of the information submitted will likely be technical in nature. For information submitted that may be in narrative form describing the incident, and perhaps the specific threat actor, the information is likely to be submitted directly by the victim. Thus, the likelihood of inaccuracies is relatively low. However, whether the information is submitted by a victim or third party, once the information is transferred to Guardian Cyber, 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 Cyber Watch specialists.

FBI reviews all cyber threat information before sending it to Cyber Watch. Upon verification, Cyber Watch provides a de-confliction check. Once the information is de-conflicted, it is sent to the Guardian Victim Assistance Unit. If appropriate, the Guardian victim notification unit can transfer the threat incident to an investigator. These multiple layers of checks and balances

ensure that only relevant information is transferred to FBI agents.

(f) **Accountability and Auditing**

15. *What methods are in place to audit access to records maintained within the system?*

Response: iGuardian is hosted and monitored by the FBI. As part of FBI's security functions, audit trails and user access are reviewed on a regular basis. As noted above, Guardian is a National Security System subject to strict audit and access procedures. All FBI employees must complete privacy training regarding the proper use of FBI information systems.

16. *Describe any oversight mechanisms that apply to the system.*

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 iGuardian 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.

Attachment B**Malware FIPPs Chart****(a) Transparency**

1. *How does the FBI incorporate the principle of transparency into Malware Investigator and information collections related to Malware Investigator?*

Response: For Privacy Act purposes, Malware login information is covered under Privacy Act SORN, DOJ-002, DOJ Computer Systems Activity and Access Records.²⁹ Malware Investigator does not generally retrieve by personally identifying information; however, the FBI's SORN for its Central Records System, FBI-002, would cover any such use beyond the Malware Investigator system.

Each Malware Investigator user's first and last name and his/her organizational identification is sent from the LEEP portal to Malware Investigator and is retained only as long as required by the System Security Plan, as mandated by the FBI Security Division. Immediately following this required retention period, this information is purged from the system. Once a submission identification number is assigned, the submitter's personal information is removed. In addition, the submitter may consent to providing his/her email address in order to facilitate sharing of suspicious file information with other users.

In order to share information, submitters must proactively opt in by setting their preferences to allow for sharing, thereby consenting. Also, this process affords submitters the opportunity to determine whether to provide their email address and to choose who will be permitted to view the technical report returned by the FBI.³⁰ Further, Malware Investigator includes a text box for users to insert comments regarding malware. The comment box instructs users to not provide PII, such as victim information, in the text box. Because of the limited collection of PII, notices regarding collection are provided at the point in time of the collection to the specific user.

In addition to email addresses that users voluntarily provide, information maintained in Malware Investigator consists of suspicious files, which may include IP addresses. These IP addresses are obtained as part of the technical analysis conducted on the malware. They identify attempted network connections the malware is trying to make. Malware Investigator's automated analysis includes executing the malware in a safe, virtual environment and identifying attempted network connections made by the malware. This information is valuable to Malware Investigator users to because it assists them in securing their system. Suspicious files may be embedded in any type of file format (*e.g.*, word, picture, or spreadsheet). In rare circumstances, the file may contain embedded PII, but the existence of PII will not be known to the system or the system users. Executable files are extracted and separated from the programs or application to help ensure that no PII contained in the host program/application is extracted by Malware Investigator. Extracted PII from executable files that is relevant to an investigation and retrieved by name or other

²⁹ DOJ-002, the DOJ Computer Systems Activity and Access Records SORN, can be located at: <http://www.gpo.gov/fdsys/pkg/FR-1999-12-30/pdf/99-33838.pdf>.

³⁰ Although users may voluntarily allow others to review the FBI's report associated with their malware submission, the system does not allow anyone but the submitter to view the initial file submission. Therefore, the FBI's report contains only technical information, and does not contain any PII that may have been inadvertently embedded in the initial submission.

personal identifier is covered under FBI-002, the Central Records System SORN. The FBI CyD and PCLU will evaluate whether a separate PIA will be needed as private sector partners become direct users of Malware Investigator.

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 FISMA certification schedule and/or when the program changes in such a way that may raise new privacy issues. Because the system is still in an early stage of development, the FBI anticipates continued oversight by FBI’s privacy attorneys to ensure that issues surrounding transparency are appropriately addressed. Specifically, as the FBI evaluates adding private sector partners as users of Malware Investigator, the FBI will re-evaluate whether the current documentation for Malware Investigator provides sufficient transparency and notice.

(b) Individual Participation

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

Response: As stated above, a Malware Investigator user’s first and last name and his/her organizational identification is sent from LEEP to Malware Investigator and is retained only as long as required by the System Security Plan, as mandated by the FBI Security Division. Immediately following this required retention period, this information is purged from the system. Once a submission identification number is assigned, the submitter’s personal information is deleted. In addition, the submitter may consent to providing his/her email address in order to facilitate sharing of the FBI’s technical reports with other users.³¹

In order to share information, submitters must proactively opt in by setting their preferences to allow for sharing, thereby consenting. Also, this process affords submitters the opportunity to determine whether to provide their email address and to choose who will be permitted to view the technical report generated by the FBI. Finally, although Malware Investigator includes a text box where users can enter information about the submission, users are advised, through a warning banner, not to enter PII in the text box.

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

Response: As stated above, although Malware Investigator includes a text box where users can enter information about the submission, users are advised, through a warning banner, not to enter PII, including victim information, in the text box. In rare circumstances, suspicious files submitted by users through Malware Investigator may contain embedded PII belonging to a third party, which may include victim information. Any victim information collected is in accordance with the civil liberty protections contained in the DOJ Use of Race Guidance. This PII is not collected directly from the individual by Malware Investigator, and thus, the third party does not have an opportunity to consent.³²

5. How does Malware Investigator ensure that the FBI CyD’s Victim Notification Process is implemented?

³¹ As stated above, only the submitter is permitted to view the initial file submission.

³² As stated above, however, executable files are extracted and separated from the programs or application to help ensure that no PII contained in the host program/application is extracted by Malware Investigator.

<p>Response: Currently, Malware Investigator’s users consist of the LE community. Thus, in most cases, the victim will not be the same entity as the Malware Investigator user, but instead the submission will be on behalf of a victim. Therefore, the LE entity who submits the information is responsible for victim notification in accordance with applicable laws and policies.</p> <p>Once Malware Investigator is open for use by the private sector community, it is likely that the private sector entity will already be aware of its status as a victim because the entity will have taken proactive steps through the use of Malware Investigator to put the FBI on notice. However, the FBI will still need to develop steps or utilize the FBI’s existing Victim Notification Process to ensure that the private sector entity is aware of the magnitude of the cyber incident and share information with the private sector entity as appropriate.</p>
<p>6. Are Malware Investigator users given the opportunity to access and correct their PII?</p>
<p>Response: Yes. Users may access and correct their first and last name and organizational identification through the process described in LEEP, and may access and correct their email address through Malware Investigator.</p>
<p>7. Are victims given the opportunity to access and correct their PII?</p>
<p>Response: Currently, victims do not have the ability to access Malware Investigator to correct information; however, as described above, victim information is not stored in Malware Investigator. Even so, when the FBI reaches out to the victim for notification purposes, the victim may provide updated information at that time. In the rare circumstance that PII is embedded in suspicious files submitted to Malware Investigator, the existence of this PII will not be known by the system or the system user.³³</p>
<p>8. Describe the mechanism provided for an individual to seek redress in the event of inappropriate access to or disclosure of their PII.</p>
<p>Response: System users may seek redress by contacting LEEP at the number listed on the login page or by contacting the Malware Investigator program office.</p>
<p>9. Describe the mechanism provided for a victim to seek redress in the event of inappropriate access to or disclosure of their PII.</p>
<p>Response: Although Malware Investigator collects very limited victim information, to the extent that the information is retrieved by name or other personal identifier, it would be covered by Privacy Act SORN, FBI-002, and thus the access and amendment provisions available under the Privacy Act are applicable to such information. If the FBI was to become aware that PII had been inadvertently embedded in the malware submitted, the FBI would take appropriate action to immediately remove the PII. Although FBI-002 is exempt from the access and amendment provisions of the Privacy Act, the FBI, in the interest of sound record-keeping, may waive such exemptions on a case-by-case basis. Moreover, FBI-002 is not exempt from the Privacy Act’s disclosure prohibition. Therefore, if an individual’s PII, was covered by the Privacy Act, 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.</p>
<p>10. What steps are taken to ensure information maintained in the system is accurate, timely, relevant, and complete?</p>
<p>Response: Once the executable files are separated from the suspicious files, the suspicious files are sent to an isolated virtual environment where technical analysis is performed to extract information. Regarding specific information about the submitter, the only information</p>

³³ As previously explained, Malware Investigator has implemented standards to ensure that potentially inadvertently embedded PII is extracted from the system.

maintained in the Malware Investigator is the submitter’s email address (if voluntarily provided), as well as the copy of the malware. The submitter’s information can all be modified through LEEP or Malware Investigator.

11. *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.*

Response: As stated above, each Malware Investigator user’s first and last name and his/her organizational is retained only long enough to generate a submission identification number for the suspicious file(s). Once a submission identification number is assigned, the submitter’s personal information is removed. In addition, the submitter may consent to providing his/her email address in order to facilitate sharing of suspicious file information with other users. In order to share information, submitters must proactively opt in by setting their preferences to allow for sharing, thereby consenting. Also, this process provides submitters with the opportunity to determine whether to provide their email address and to choose who will be permitted to view their file and the associated report returned by the FBI. Users are able to correct inaccurate first and last names through LEEP, and can correct inaccurate email addresses directly through Malware Investigator.

Further, although Malware Investigator includes a text box where users can enter information about the submission, users are advised, through a warning banner not to enter PII in the text box. Finally, in rare circumstances, malware submitted by users through Malware Investigator may contain embedded PII belonging to a third party. As this PII is not collected directly from the individual victim by Malware Investigator, the third party does not currently have an opportunity to provide consent. However, in the future, Malware Investigator will permit private sector partners, which in most cases will be victims themselves, to submit information directly to Malware Investigator. The PII that may be embedded in a suspicious file is extracted from the suspicious file and analyzed in another system. There is no technical method for Malware Investigator users to access this PII and/or manipulate the PII once submitted to Malware Investigator.

(c) Purpose Specification

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

Response: The specific purpose for the maintenance of user information within Malware Investigator is to facilitate information sharing and permit account authentication and access, as well as to facilitate contact between other Malware Investigator users. Given the technical nature of the malware submissions, and because no PII is analyzed, it is difficult to predict a scenario in which the FBI could ascertain that the information submitted to Malware Investigator could be evidence of another crime unrelated to the purpose for the submission. By its very nature, this type of technical information would be relevant to cyber matters and would be retained with other malware submissions as a resource for cyber investigations. The FBI is not required to restrict this information to only cybersecurity purposes; however, as a practical matter, submissions to Malware Investigator generally relate only to cyber matters.

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

Response: Currently, users of Malware Investigator are LE partners. The FBI depends on the LE partners to ensure that there is a valid basis to collect the information submitted to the FBI. However, if the FBI determines that action beyond analyzing the suspicious file and reporting back results is necessary, the FBI will follow its usual case management process as outlined in the Sentinel PIA to ensure that collection of the information submitted was valid.

(d) Data Minimization

14. *Describe the data elements that are relevant and necessary and the retention and disposal of those data elements.*

Response: As stated above, Malware Investigator collects only a limited amount of PII. Each Malware Investigator user's first and last name and his/her organizational identification is sent from LEEP to Malware Investigator so that suspicious files submitted by a user are tagged with a submission identification number. Once a submission identification number is generated, the submitter's personal information is deleted. In addition, the submitter may consent to providing his/her email address in order to facilitate sharing of the FBI's technical report with other users.³⁴ In order to share this information, submitters must proactively opt in by setting their preferences to allow for sharing, thereby consenting. Also, this process provides submitters with the opportunity to determine whether to provide their email address and to choose who will be permitted to view the associated report returned by the FBI. Further, Malware Investigator includes a text box for users to insert comments regarding malware. The comment box includes instructions advising users not to enter PII, including victim information, in the text box. Because of the limited collection of PII, notices regarding collection are provided at the point in time that the information is collected from the specific user.

In addition to user email addresses (if voluntarily provided), information maintained in Malware Investigator consists of suspicious files, which may include IP addresses that are acquired through various sources, such as through seizure of hardware pursuant to a search warrant, IC collections, commercial collections, and reporting by corporate entities or private citizens. Suspicious files may be embedded in any type of file format (*e.g.*, word, picture, and spreadsheet). The file may contain embedded PII, but it will not be extracted from the file for analysis or maintained within Malware Investigator. Executable files are extracted and separated from the programs or application to help ensure that no PII contained in the host program/application is introduced to Malware Investigator.

Thus, the amount of PII collected from the system user is limited to information necessary to facilitate collaboration. The user's name and organization are only retained until a submission identification number can be generated. Therefore, it is the submission identification number, not the user's name and organization that is entered with the host program/application into Malware Investigator. Email addresses (if voluntarily provided) are entered into Malware Investigator, and are maintained in accordance with a Records Management Division retention schedule.

Presently, all technical malware submissions are retained for the life of the Malware Investigator system, as set forth in the System Security Plan and current Records Management Division requirements. Because Malware Investigator is in its initial stages, these data retention issues are still being evaluated. In 2015, the FBI plans to start development on a more comprehensive data retention plan. The FBI will work with the National Archives and Records Administration (NARA) for a schedule to establish an appropriate records retention and disposition schedule for records that may be contained in Malware Investigator. While this schedule is being developed, for any data in Malware Investigator, the FBI will follow the schedules set for current record categories.

³⁴ As stated above, the system does not allow anyone but the submitter to view the initial file submission.

(e) Use Limitation
<p>15. <i>Describe steps taken to ensure the use of PII is limited to the purpose(s) specified in applicable notices.</i></p>
<p>Response: As stated above, Malware Investigator only permits users to perform limited functions, which consist of logging into the system,³⁵ submitting suspicious files, describing files in a text box,³⁶ and sharing such information with other users.</p> <p>As an analytic tool used to gain technical information about the functionality of a malware sample, submitting suspected malware does not constitute reporting a cyber event. Rather, the FBI views it as asking to receive technical information about a file. Therefore, the FBI does not track these submissions back to the submitter, and there is no mechanism available for agents to even contact a submitter if the sample was of interest to the FBI (unless the submitter has voluntarily provided an email address for collaboration purposes). Similarly, Malware Investigator does not make a determination about whether a submitted file is a cyber threat. It is actually up to the submitter to make that determination based on technical feedback.</p> <p>Additionally, all files submitted to Malware Investigator are stripped down to executables. Only executables files are analyzed. Thus, the only information remaining for users is technical information that does not contain PII. The original submission is not available for review by any users, so there is no PII available to be shared for law enforcement purposes. Accordingly, this helps to ensure that the use of PII is limited to the purpose specified in applicable notices.</p> <p>Thus, it is unlikely that the FBI could observe through analysis that the information submitted to Malware Investigator may be evidence of another crime unrelated to the purpose for the submission. Although this has not yet occurred, if there is such a future scenario, the FBI follows applicable laws and policies. The FBI will continue to evaluate its information sharing policies, as well as monitor and review its information sharing policies relating to cybersecurity law enforcement.</p>
(f) Data Quality and Integrity
<p>16. <i>What steps are taken to ensure that data is accurate, timely, relevant, and complete?</i></p>
<p>Response: As stated above, the user’s first and last name and his/her organizational identification is sent from LEEP to Malware Investigator so that suspicious files are tagged with the submitter’s information. In addition, the submitter may choose to provide his/her email address in order to facilitate sharing of the FBI’s technical report with other users. Because this information is submitted directly by the user, there is a low risk of inaccurate data. Further, users are able to correct inaccurate first and last names through LEEP, and can correct inaccurate email</p>

³⁵ There is no requirement for a private sector entity to submit files to Malware Investigator. Currently, access to the service can only be gained by logging in to the LEEP portal, which has a banner to clarify that there is no reasonable expectation of privacy. The banner contains the following notice:

You are accessing a U.S. Government information system. . . . By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

³⁶ Private sector entities are advised, through a warning banner, not to enter PII.

addresses directly through Malware Investigator.

Finally, malware submitted by users through Malware Investigator may contain embedded PII belonging to a third party. Currently, this PII is not collected directly from the individual victim by Malware Investigator, and thus, the third party does not have an opportunity to verify accuracy. However, if the FBI is notified that PII has been submitted to Malware Investigator, there are procedures in place, as previously described. In the future, Malware Investigator will permit private sector partners, which in most cases will be victims, to submit information directly to Malware Investigator.

The PII that may be embedded in a suspicious file is extracted from the suspicious file. There is no way for Malware Investigator users to access this PII and/or manipulate the PII once submitted to Malware Investigator. Thus, the risk of inaccuracy is low. Further, because users are submitting information for the purpose of receiving an analysis back from the FBI, and because the data is largely technical in nature, the likelihood of a user intentionally submitting inaccurate information is low.

(g) Security

17. Describe any safeguards that are in place to ensure the continued security of data associated with this system.

Response: FBI information systems used to process and store sensitive information undergo certification and accreditation processes to verify that the system provides confidentiality, integrity, and availability of information. As part of this stage, processes such as vetting for LEEP users and subsequent Malware Investigator users are established. There are auditing mechanisms to ensure users appropriately handle information, network monitoring to protect from intrusions, and other programs are also in place to protect the system.

(h) Accountability and Auditing

18. What methods are in place to audit access to records maintained within the system?

Response: Malware Investigator is hosted and monitored by the FBI. As part of FBI's security functions, audit trails and user access can be reviewed on a regular basis.

19. Describe any oversight mechanisms what apply to the system.

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 Malware Investigator is still in its beginning stages, privacy attorneys are embedded within the Cyber Division 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.

PART V: DEPARTMENT OF COMMERCE



Executive Summary

For the reporting period of August 1, 2013 to September 30, 2014, the Department of Commerce (DOC) Chief Privacy Officer (CPO)/ Senior Agency Official for Privacy (SAOP) completed a Privacy Assessment examining DOC activities performed pursuant to Executive Order (E.O.) 13636 – Improving Critical Infrastructure Cybersecurity. E.O. 13636 directs federal departments and agencies to establish, expand, or prioritize a number of activities to improve cybersecurity for the United States (U.S.) critical infrastructure. Section 5 of the E.O. requires department and agency Senior Agency Officials for Privacy and Civil Liberties³⁷ (SAOP/CLs) to incorporate privacy and civil liberties protection into such activities, and to conduct assessments of those activities based on Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks.

The DOC manages satellite imagery and meteorological forecasting critical infrastructure systems/ services owned and operated by the National Oceanic and Atmospheric Administration (NOAA), but relies on the Department of Homeland Security (DHS) to perform all cybersecurity and threat intelligence information sharing activities directed by Section 4 of the E.O. This Privacy Assessment was therefore limited to DOC specific Section 7 and Section 8 “Cybersecurity Framework” development related activities performed by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA).

The DOC CPO/ SAOP’s observations and findings are as follows:

1. Section 7(a) of the E.O. directs the NIST to lead the development of a Cybersecurity Framework in collaboration with industry. This required NIST’s collection and processing of support contractor and conference/workshop registration related personally identifiable information (PII). Additionally, it required storage of PII submitted voluntarily during the public comment period on the NIST Information Technology (IT) systems.

In all cases, the NIST ensured implementation of appropriate IT security and privacy protections. Accordingly, the level of privacy risk presented by these activities is Low³⁸ and in adherence with FIPPs. No civil liberties risks/ impacts were presented by the NIST collection and processing of subject PII; thus none were assessed.

2. Section 7(c) of the E.O. requires the Cybersecurity Framework to include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties. This required NIST inclusion of the section entitled “Methodology to Protect Privacy and Civil Liberties (P/CL Methodology).”

The P/CL Methodology section appropriately acknowledges that privacy and civil liberties impacts may arise as part of cyber security operations envisioned under the Cybersecurity Framework. It represents private sector consensus on a general set of methodologies, considerations, and processes to address privacy and civil liberties implications of cybersecurity

³⁷ The DOC does not have a designated Civil Liberties Officer.

³⁸ A Low risk is one in which the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organization assets or individuals.

operations under the Cybersecurity Framework. As the consensus document directed by the E.O., the P/CL Methodology of the voluntary Cybersecurity Framework meets these purposes.

3. Section 8(d) of the E.O. directs the Secretary of Commerce to evaluate a set of incentives designed to promote participation in a voluntary program, which will be established by the Secretary of Homeland Security to support the adoption of the Cybersecurity Framework. On behalf of the Commerce Secretary, this required the NTIA issuance of a Federal Register notice of inquiry entitled “Incentives to Adopt Improved Cybersecurity Practices.” NTIA also released two reports which outlined recommendations and discussions on incentives for critical infrastructure owners and operators to join a voluntary Cybersecurity program.

These NTIA led activities required no PII collection and involved no privacy or civil liberties risks/impacts.

All activities required under E.O. 13636 have appropriately incorporated privacy and civil liberties protections. No further Privacy Assessment activity subject to Section 5 reporting requirements is anticipated.

1. Introduction

The national and economic security of the United States (U.S.) depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (E.O.) - Improving Critical Infrastructure Cybersecurity, dated February 12, 2013. The E.O. directs federal departments and agencies to establish, expand, or prioritize a number of activities to improve cybersecurity for the United States (U.S.) critical infrastructure, including the development of a framework (the “Cybersecurity Framework”) to reduce cybersecurity risks to critical infrastructure and to assist organizations responsible for critical infrastructure services with managing cybersecurity risk.

Section 5 of the E.O. requires department and agency Senior Agency Officials for Privacy and Civil Liberties³⁹ (SAOP/CLs) to incorporate privacy and civil liberties protection into all activities performed under the E.O., and to conduct assessments of those activities based on Fair Information Practice Principles (FIPPs) and other applicable policies, principles and frameworks.

For the reporting period of August 1, 2013 to September 30, 2014, the Department of Commerce (DOC) Chief Privacy Officer (CPO)/ Senior Agency Official for Privacy (SAOP) completed a Privacy Assessment examining “Cybersecurity Framework” development activities performed by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). The DOC performed no critical infrastructure related cybersecurity or threat intelligence information sharing with U.S. private sector entities pursuant to the E.O. during this period. In addition, none are required or expected to be undertaken by the DOC in any future reporting period.

1.1 Protection of Critical Infrastructure Systems/ Services

Critical infrastructure systems/ services within DOC are operated/ performed by the National Oceanic Atmospheric Administration (NOAA). They include the following Primary Mission Essential Functions (PMEFs) which support National Essential Functions (NEFs).

1. Satellite imagery: Collect and provide the Nation with critical intelligence data, imagery, and other essential information for predictive environmental and atmospheric modeling systems and space-based distress alert systems by operating NOAA-controlled satellites, communications equipment, and associated systems.
2. Meteorological forecasts: Provide the Nation with environmental forecasts, warnings, data, and expertise critical to public safety, disaster preparedness, all-hazards response and recovery, the national transportation system, safe navigation, and the protection of the Nation’s critical infrastructure and natural resources.

NOAA implements a number of Cybersecurity measures to protect critical infrastructure services in NOAA networks, systems, computers, programs, and data from cyber-attack, damage, and unauthorized access. They encompass establishment, coordination, and implementation of a functional body of technologies, processes, architecture and practices which include the following:

³⁹ The DOC does not have a designated Civil Liberties Officer.

1. TIC – Trusted Internet Connection

Trusted Internet Connection (TIC) Access Provider (TICAP) services are grouped together in a physical TIC stack at each of the four NOAA TICAP Locations and provide required TIC services to address the 60 Security Controls.

2. N-CIRT – NOAA Computer Incident Response Team

The N-CIRT's primary mission is to respond to computer security incidents. This includes identifying incidents, and employing countermeasures to defend, contain, and recover from incidents.

3. SOC – Security Operations Center

The NOAA Security Operations Center (SOC) improve the Agency's Incident Detection and Response capabilities, provides alerts and notifications to general and specific threats, and provide reporting to senior agency management, cyber security personnel, and Cyber Incident Responders.

4. ESS – Enterprise Security Services

The NOAA Enterprise Security Services (ESS) provides web content filtering, vulnerability management and continuous monitoring

5. ECMO - Enterprise Continuous Monitoring Operations

Real time visibility, control, and management over all IT endpoints including devices including routers, switches, servers, desktops, and laptops

The E.O. establishes that it is the policy of the U.S. Government to increase the volume, timeliness, and quality of critical infrastructure related cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. The DOC and NOAA however, rely on the Department of Homeland Security (DHS) to perform all Section 4 required sharing of cybersecurity and threat intelligence information sharing with U.S. private sector activities of this E.O.

1.2 Cybersecurity Framework Development Activities

The Cybersecurity Framework development activities performed within the DOC during this second reporting period were led by the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). This report documents privacy and civil liberties assessment findings associated with those activities, and includes an assessment of the Privacy and Civil Liberties Methodology (P/CL) section of the Cybersecurity Framework.

(The report on privacy and civil liberties assessment findings associated with E.O. 13636 activities performed within the DOC during the first reporting period was included as [Part V of the Department of Homeland Security report on Executive Order 13636 Privacy and Civil Liberties](#), published on April 10, 2014.)

2. Overview of the Privacy Organization and Processes

DOC is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information (PII) is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the

developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

The Office of Privacy and Open Government (OPOG) within the Office of the Secretary (OS) provides oversight and management of the DOC privacy program. OPOG is headed by the DOC Chief Privacy Officer (CPO) who reports to the Chief Financial Officer and Assistant Secretary for Administration (the CFO/ASA) and the Deputy Assistant Secretary for Administration.

The CPO serves as the Department's key policy advisor on implementing the Privacy Act of 1974; and the privacy provisions of the Federal Information Security Management Act (FISMA) and of the E-Government Act of 2002. In addition, the CPO represents the Department on the National Science and Technology Council, Federal Chief Information Officer (CIO) Council Privacy Committee and does the following:

- Serves as the Department's senior policy authority on matters relating to the public disclosure of information, and advises on privacy issues related to informed consent, disclosure risk, and data sharing.
- Develops and oversees implementation of Department-wide policies and procedures relating to the Privacy Act, and assures that personal information contained in Privacy Act systems of records is handled in compliance with its provisions.
- Communicates the Department's privacy vision, principles and policies internally and externally; advises on and takes steps to address any deficiencies related to privacy-related legislation and regulations.
- Advocates strategies for data and information collection and dissemination, and ensures Departmental privacy policies and principles are reflected in all operations.
- Ensures Departmental policies and procedures regarding information protection are compliant with statutory and government-wide policy requirements, verifies bureau adherence to relevant information protection policies and procedures, and continually strives to identify and implement privacy best practices.
- Coordinates the Departmental process for reviewing and approving Privacy Impact Assessments (PIAs) in connection with the E-Government.
- Manages the process for reviewing and approving privacy programs as part of the Office of Management and Budget (OMB) budget process, and works with the CIO to ensure that the FISMA certification and accreditation process for new and existing systems appropriately addresses privacy-related issues.
- Ensures the appropriate training and education regarding privacy laws, regulations, policies and procedures concerning the handling of personal information are afforded to DOC employees and contractors.
- Facilitates and negotiates agreements with senior management, and establishes relationships with partners in private industry and other federal agencies to foster the development and sharing of privacy-related best practices.
- Serves as the Senior Agency Official for Privacy (SAOP) and is advised by majority vote of Executive members of the DOC Privacy Council which includes the Deputy Assistant Secretary for Administration, the CIO, and the Assistant General Counsel for Administration.

- Serves as Chair of the DOC Privacy Council which includes the DOC Bureau / Operating Unit Chief Privacy Officers (BCPOs) from across the Department. The DOC Privacy Council works to strengthen Department privacy policies to ensure that they reflect the goals, values, and policies that the Department advocates.

The DOC privacy program is implemented within its Bureaus and Operating by the DOC Bureau Chief Privacy Officers (BCPOs). The BCPOs manages the individual Bureau/ Operating Unit (BOU) portions of the privacy program. The CPO partners with the Office of Chief Information Officer (OCIO) to ensure all aspects of the privacy program are incorporated into the Department's enterprise infrastructure, IT, and IT security program.

3. Overview of the Privacy Assessment Methodology

The DOC CPO/ SAOP completed a Privacy Assessment review of Cybersecurity Framework development activities and products performed/ published by the NIST and NTIA. The assessment was conducted by incorporating results and recommendations from the Privacy Assessment of Cybersecurity Framework development activities completed during the first reporting period, and evaluating any changed and new activities / products against the Fair Information Practice Principles (FIPPs) as appropriate, as well as the privacy provisions of the FISMA related to conduct of PIAs. The assessment included an examination of the following:

- [NIST Cybersecurity Framework, Updates and Activities:](#)
 - [Cybersecurity Framework version 1.0;](#)
 - [Update on the Cybersecurity Framework;](#) and
 - [Additional Cybersecurity Framework Workshops.](#)
- [NTIA Issuances and Reports:](#)
 - [Notice of Inquiry \(NOI\): Incentives To Adopt Improved Cybersecurity Practices](#)
 - [Comments on Incentives To Adopt Improved Cybersecurity Practices NOI](#)
 - [Recommendations To The President On Incentives For Critical Infrastructure Owners And Operators To Join A Voluntary Cybersecurity Program;](#) and
 - [Discussions Of Recommendations To The President On Incentives For Critical Infrastructure Owners And Operators To Join A Voluntary Cybersecurity Program;](#)

4. Summary Description of the E.O. Implementation Activities Assessed

a. NIST Collection and Processing of PII for the Cybersecurity Framework Development Workshop

Section 7(a) of the E.O. directs the NIST to lead the development of a Cybersecurity Framework in collaboration with industry. Accordingly, NIST issued Requests for Information (RFIs), received public comments, and held a series of public workshops the majority of which were conducted during the first reporting period. One additional workshop however was conducted during this reporting period. Conduct of the workshop involved the collection and processing of support contractor and conference/workshop registration related PII that are subject to privacy protections afforded by the Privacy Act of 1974 and the FISMA. The PIAs for IT systems used by NIST to collect and store the PII were reviewed to ensure the IT security and privacy protections required to protect stored PII were in place and functioning as intended.

b. The Privacy and Civil Liberties Methodologies Section of the Cybersecurity Framework

Section 7(c) of the E.O. requires the Cybersecurity Framework to include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties. This required NIST inclusion of the section entitled “Methodology to Protect Privacy and Civil Liberties (P/CL Methodology).”

The P/CL Methodology section was evaluated to determine if it appropriately identified that privacy and civil liberties impacts may arise as part of cyber security operations envisioned under the Cybersecurity Framework, and whether it represents private sector consensus on a general set of methodologies, considerations, and processes to address privacy and civil liberties implications of cybersecurity operations under the Cybersecurity Framework.

4.3 NTIA Development of “Incentives to Adopt Improved Cybersecurity Practices”

Section 8(c) of the E.O. directs the Secretary of Commerce to evaluate a set of incentives designed to promote participation in a voluntary program to be established by the Secretary of Homeland Security to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities of the Cybersecurity Framework being developed by the NIST. The NTIA with NIST issued a Federal Register NOI entitled “Incentives to Adopt Improved Cybersecurity Practices.” In addition, NTIA released two reports about incentives for adoption of the cybersecurity framework, which were based on the notice of inquiry. These reports outlined the recommendations and discussions on incentives for critical infrastructure owners and operators to join a voluntary Cybersecurity program. These activities and reports were reviewed for privacy and civil liberties risks/ impacts. It was determined that none were presented.

5. Detailed Privacy and Civil Liberties Assessment

5.1 Analysis of the NIST Collection and Processing of PII for the Cybersecurity Framework Development Workshop

The Cybersecurity Framework was developed by NIST employees and contractors through a series of meetings with and requests for information from the public, followed by draft documents, and receipt of draft document comments from the public. These activities involved the collection and processing of support contractor and conference/workshop registration related PII that are subject to privacy protections afforded by the Privacy Act of 1974 and the FISMA.

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

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

The NIST conducted only one Cybersecurity Framework development workshop during this reporting period. NIST followed the same procedures used for the previous workshops and which were assessed against the FIPPs as follows.

Transparency

Transparency objectives were fully met with NIST creation of the Cybersecurity Framework public website at <http://www.nist.gov/itl/cyberframework.cfm>. This website provides access to all supporting documents, links to current and previous workshops/events, framework development, the RFIs, and the NOIs. The NIST engaged the public for comments using the RFI process which required publication in the Federal Register for each round of comments. The 45-day public comment period opened on October 29, 2013, for the preliminary Framework in the Federal Register. Complete details about the comment process and period can be found at <https://www.federalregister.gov/articles/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework>. All comments have been posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html, without change, or redaction, and commenters are reminded not to include information they do not wish to be posted (e.g., personal or business information).

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

Individual Participation

Individual participation in the Cybersecurity Framework activities was purely voluntary. The PII collected as part of the process was limited to the conference/workshop participant's name, company name, e-mail address, and public comments which sometimes included PII. The NIST met individual participation objectives, by publishing conference/workshop registration information at each workshop. NIST also published comments collected during the public comments phase. This afforded participants an effective mechanism for appropriate access, correction, and redress regarding the use of PII.

Purpose Specification

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

Data Minimization

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

Use Limitation

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

Data Quality and Integrity

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

Security

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

Accountability and Auditing

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

In all cases, the NIST ensured implementation of appropriate IT security and privacy protections. Accordingly, the level of privacy risk presented by these activities is Low⁴⁰ and in adherence with FIPPs. No civil liberties risks/impacts were presented by NIST collection and processing of subject PII; thus none were assessed.

5.2 Analysis of the Privacy and Civil Liberties Methodologies Section of the Framework

NIST published a preliminary version of the Cybersecurity Framework (the preliminary Framework) on October 22, 2013 and a final version entitled "Framework for Improving Critical Infrastructure Cybersecurity" (the final Framework) on February 14, 2014. The Framework relies on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk, and is a risk-based approach comprised of the following three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

- I. The Framework Core is a set of cybersecurity activities and references that are common across critical infrastructure sectors organized around particular outcomes. The Framework Core consists of five functions that can provide a high-level, strategic view of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key categories and subcategories for each of these

⁴⁰ A Low risk is one in which the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organization assets or individuals.

- functions, and matches them with informative references, such as existing standards, guidelines, and practices for each Subcategory.
- II. Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from partial (Tier 1) to adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
 - III. A Framework Profile (“Profile”) represents the outcomes that a particular system or organization has achieved, or is expected to achieve, as specified in the Framework Categories and Subcategories. Profiles are also used to identify opportunities for improving cybersecurity by comparing a “Current” Profile with a “Target” Profile.

The Privacy and Civil Liberties Methodology (P/CL Methodology) is provided in Section 3.5 of the final Framework. The P/CL Methodology describes a methodology as required by the Executive Order to address individual privacy and civil liberties implications that may result from cybersecurity operations. It provides general guidance on privacy and civil liberties considerations and risks that may arise when personal information is used, collected, processed, maintained, or disclosed in connection with organizations cybersecurity operations.

The P/CL Methodology notes that government and agents of the government which own or operate critical infrastructure have a direct responsibility to protect civil liberties arising from cybersecurity activities, as well as to have in-place privacy law compliant processes. It provides that non-government owners and operators of critical infrastructure who voluntarily adopt the Cybersecurity Framework may address privacy implications by considering how their cybersecurity program might incorporate privacy principles such as: *data minimization* in the collection, disclosure, and *retention* of personal information material related to the cybersecurity incident; *use limitations* outside of cybersecurity activities on any information collected specifically for cybersecurity activities; *transparency* for certain cybersecurity activities; individual *consent and redress* for adverse impacts arising from use of personal information in cybersecurity activities; *data quality, integrity, and security*; and *accountability and auditing*. The Cybersecurity Framework additionally identifies methods to incorporate privacy risk management based on existing standards, guidance, and best practices. The incorporation of these methods into the cybersecurity activities of an organization will be based on the risk acceptance level defined by the organization. These suggested considerations encourage organizations which voluntarily use the Cybersecurity Framework to ensure consistency of cybersecurity operations with the FIPPs to mitigate privacy impacts. This version of the P/CL Methodology however is not prescriptive because the Cybersecurity Framework, as directed by the E.O., incorporates voluntary consensus standards and industry best practices to the fullest extent possible. It is not a compliance document. Non-government owners and operators of critical infrastructure may determine that they already implement comparably effective P/CL methodologies.

The P/CL Methodology section of the final Framework is substantially different from the P/CL Methodology provided in the preliminary Framework. The preliminary Framework provided the P/CL Methodology as a separate Appendix B which was organized by Function and Category to correspond with the Framework Core. It was based on FIPPS, presented methodologies to address P/CL considerations associated with the deployment of cybersecurity activities, and mapped each to specific informative reference documents. NIST found that the separate P/CL Methodology provided as Appendix B of the preliminary Framework did not generate sufficient support through the comments to be included in the final Framework. NIST reported that while stakeholders said that they see the value of guidance relating to privacy, many comments stated a concern that the methodology did not reflect consensus private sector practices and therefore might limit use of the Framework. There was specific concern that a P/CL methodology that attempts to map the FIPPS to most features of the Framework would be difficult for organizations to follow and risks discouraging organizations from committing to use the Framework. Many commenters also stated their belief that privacy considerations should be fully integrated into the Framework Core. Additionally, commenters expressed support for an alternative methodology proposed by stakeholders and discussed publicly at the 5th NIST Framework Workshop in November.⁴¹

The final Framework version of the P/CL Methodology at section 3.5 is the product of NIST's collaboration with stakeholders to achieve consensus. Unlike the preliminary Framework's Appendix B, the section 3.5 P/CL Methodology is not organized by Function and Category to correspond with the Framework Core, and does not attempt to directly associate specific FIPPS based methodologies with the deployment of cybersecurity activities. Accordingly, a revised DOC P/CL assessment approach was required. The planned assessment as referenced on page 3 of last year's report, centered on using specific cybersecurity information and cyber threat intelligence sharing scenarios to test whether Appendix B methodologies were appropriately mapped to effectively assist with identifying and mitigating P/CL risks associated with use of the Cybersecurity Framework. The final Framework version of the P/CL Methodology could not be assessed this way.

This year's privacy assessment consisted of the P/CL Methodology section of the Cybersecurity Framework consisted of reviewing it to ensure it acknowledges that privacy and civil liberties impacts may arise as part of cybersecurity operations envisioned under the Cybersecurity Framework, and to determine whether it represents private sector consensus on a general set of methodologies, considerations, and processes to address privacy and civil liberties implications of cybersecurity operations under the Cybersecurity Framework which may differ by sector, and over time. As the consensus document directed by the E.O., the P/CL Methodology of the voluntary Cybersecurity Framework meets these purposes.

⁴¹ For the initial submission see: http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf. A webcast of the privacy panel at the 5th workshop can be found here: <http://www.nist.gov/itl/csd/5th-cybersecurity-framework-workshop-november-14-15-2013.cfm>

5.3 Analysis of the NTIA Development of “Incentives to Adopt Improved Cybersecurity Practices”

To support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities of the Cybersecurity Framework, the NTIA with NIST issued a Federal Register notice of inquiry entitled “Incentives to Adopt Improved Cybersecurity Practices.” In addition, NTIA released two reports incentives for adoption of the cyber security framework, which were reports based on the notice of inquiry. These reports outlined the recommendations and discussions on incentives for critical infrastructure owners and operators to join a voluntary Cybersecurity program. The following activities and reports were reviewed for privacy and civil liberties risks. It was determined that none were presented.

- I. The NOI which was issued on March 28, 2013, [Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices](#) with an end of comment period of April 29, 2013. All of the comments can be found on the NTIA website at [Comments on Incentives to Adopt Improved Cybersecurity Practices NOI](#).
- II. NTIA’s analysis of the comments and compilation of the final reports which were performed during the period of May through July and which culminated into the issuance of two reports on August 6, 2013.
- III. The NTIA reports which can be found on the NTIA website at [Discussion and Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program](#).

6. Summary of Findings and Recommendations

The DOC CPO / SAOP’s observations and findings are as follows:

1. Section 7(a) of the E.O. directs the NIST to lead the development of a Cybersecurity Framework in collaboration with industry. This required NIST’s collection and processing of support contractor and conference/workshop registration related personally identifiable information (PII). Additionally, it required storage of PII submitted voluntarily during the public comment period on NIST Information Technology (IT) systems.

In all cases, the NIST ensured implementation of appropriate IT security and privacy protections. Accordingly, the level of privacy risk presented by these activities is Low⁴² and in adherence with FIPPs. No civil liberties risks/ impacts were presented by NIST collection and processing of subject PII; thus none were assessed.

2. Section 7(c) of the E.O. requires the Cybersecurity Framework to include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties. This required NIST inclusion of the section entitled “Methodology to Protect Privacy and Civil Liberties (P/CL Methodology).”

The P/CL Methodology section appropriately acknowledges that privacy and civil liberties impacts may arise as part of cyber security operations envisioned under the Cybersecurity

⁴² A Low risk is one in which the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organization assets or individuals.

Framework. It represents private sector consensus on a general set of methodologies, considerations, and processes to address privacy and civil liberties implications of cybersecurity operations under the Cybersecurity Framework. As the consensus document directed by the E.O., the P/CL Methodology of the voluntary Cybersecurity Framework meets these purposes.

3. Section 8(c) of the E.O. directs the Secretary of Commerce to evaluate a set of incentives designed to promote participation in a voluntary program, which will be established by the Secretary of Homeland Security to support the adoption of the Cybersecurity Framework. On behalf of the Commerce Secretary, this required the NTIA issuance of a Federal Register notice of inquiry entitled “Incentives to Adopt Improved Cybersecurity Practices.” NTIA also released two reports which outlined recommendations and discussions on incentives for critical infrastructure owners and operators to join a voluntary Cybersecurity program.

These NTIA led activities required no PII collection and involved no privacy or civil liberties risks/ impacts.

7. Conclusion

All activities required to be performed by the DOC under E.O. 13636 have appropriately incorporated privacy and civil liberties protections. No further Privacy Assessment activity subject to Section 5 reporting requirements is anticipated.

This reporting period’s P/CL report completes the review and assessment of DOC activities involving privacy and civil liberties risks in the development and publication of the Cybersecurity Framework.

PART VI: 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. 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.

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.

Last year's report, the first under EO 13636, was a summary of the preliminary start-up activities agencies undertook as per their responsibilities under EO 13636. 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 21¹, HHS was designated the Sector-Specific Agency for the Healthcare and Public Health Sector, as well as the Co-Sector Specific Agency for the Food and Agriculture Sector alongside the Department of Agriculture.

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

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

While HHS is not an owner or operator of critical infrastructure, as defined in EO 13636, it assists parties in protecting their systems from unauthorized access, exploitation, or harm by sharing its 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 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. As part of its FY15 initiatives, HHS will continue 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:

Risk Management Program:

The expanding quantity and types of data collected, the adoption of new technologies, and the increasing complexity of regulations have increased the potential risks to individual privacy. HHS counters that trend by incorporating risk management into every phase of system and program development. As noted in last year's report, HHS's risk management programs raise awareness among employees and leadership regarding the standards for data safety. Risk management improves safety and security by instituting a training framework, compliance assessments, and vulnerability repairs. HHS will continue developing a workforce plan to include privacy-focused training for both the general end-users, as well as role-based training for those with increased privacy and security-related responsibilities. Promoting staff awareness of appropriate standards for collection, use, sharing, and disclosure of PII improves HHS's safety and security and reduces the possibility of errors in policy, behavior, or technology that could lead to undesirable privacy outcomes.

Coordination of Privacy and Civil Liberties:

HHS is establishing an initiative to create an ad-hoc response team, comprised of HHS privacy and program officials that will define protocols to mitigate and prevent risks to individuals' privacy and civil liberties. The response team will be comprised of representatives from the Office of the Assistant Secretary for Planning and Evaluation (ASPE), the Office of the Chief Information Officer (OCIO), the Office of the General Counsel (OGC), the Office for Civil Rights (OCR), and the Office of Security and Strategic Information (OSSI). The response team will address issues that require immediate consideration and response, including potential gaps in the protection of individuals' privacy and civil liberties relating to the collection, use, storage, and sharing of PII and protected health information (PHI). OCR will continue to function as an external-facing division, receiving Health Insurance Portability and Accountability Act (HIPAA) and civil rights complaints from members of the transparency of HHS's methods for safeguarding individuals' PII and PHI.

The purpose of these coordination efforts is to anticipate future risks, develop a response plan, (or have the security tools necessary to quickly and effectively produce a comprehensive response plan), mitigating risks to individuals' privacy and civil liberties. The coordination program will become a fundamental tool for HHS's remediation of privacy and civil liberties issues.

Cybersecurity Working Group:

This group is chaired by the Chief Information Officer (CIO) and coordinates cybersecurity activities across the Department. The Assistant Secretary for Preparedness and Response (ASPR), the Food and Drug Administration (FDA), and the OCIO lead the Department's implementation cybersecurity activities. OSSI, ASPE, OGC, and the Office of the National Coordinator for Health Information Technology (ONC) support and provide advice, in

accordance with their expertise, on cyber and kinetic threats, proposed revisions to privacy policy, the continuous evolution of health information technology, and monitoring of new and emerging legal matters. These offices, as well as other Departmental components, if needed, meet periodically to collaborate and coordinate EO 13636 implementation.

In addition to its participation in this working group, HHS is also represented on the Interagency Task Force (ITF) and the ITF's Assessments Working Group. Given that HHS does not own or operate critical infrastructure, as defined in EO 13636, its role in these groups has been limited to participation and review. However, HHS expects to assume more of an advisory role, sharing its security and information management tools and best practices to strengthen the government's overall cybersecurity resiliency.

Cybersecurity Information Sharing:

In line with the goals of EO 13636, HHS seeks to maximize the utility of cyber threat information sharing among its fellow government agencies, as well as with its external stakeholders and partners. In order to facilitate information sharing, HHS participates in an interagency working group charged with developing reporting instructions and processes for disseminating reports that will facilitate an increase in the volume, timeliness, and quality of cyber threat information shared by government agencies with private sector entities. HHS's participation has been limited to reviewing and commenting on draft products developed by DHS, in close coordination with the Department of Justice (DOJ) and the Office of Director of National Intelligence (ODNI), and disseminating the information for interagency review; however, HHS expects to increase its involvement and collaboration, i.e., HHS and DHS have signed a memorandum of agreement to allow for a HHS Liaison Officer to represent HHS and the Healthcare and Public Health Sector, as well as the Food and Agriculture Sector on the DHS National Cybersecurity and Communications Integration Center Floor. Information sharing provides the foundation upon which HHS may develop additional information management tools.

Cybersecurity Framework:

As per EO 13636, the National Institute of Standards and Technology (NIST), within the Department of Commerce, is leading the development of the "Improving Critical Infrastructure Cybersecurity Framework" that includes standards, methodologies, procedures, and processes that can be used by entities can use to address cyber risk. In FY 14, HHS has been actively engaged with NIST on the continued development of the Framework.

Voluntary Critical Infrastructure Cybersecurity Program:

Reaching a consensus on the definition and scope of privacy information management has been a key challenge behind the development of the Framework. In order to combat gaps in current privacy practices, NIST began conducting a series of open forum working groups and recently released a formal Request for Information (RFI) to gain input from industry, academia, government, and the public, on the formulation of voluntary standards, guidelines, and best practices. NIST has hosted privacy workshops on a quarterly basis to develop strategies to

mitigate the impact of cybersecurity activities on an individual's privacy or civil liberties. Last year, HHS limited its participation to providing review and comment on draft products; however, this year HHS expects to increase its involvement in NIST's activities. Additionally, HHS will collaborate with private and public sector entities to improve the protection of individuals' privacy and civil liberties within the voluntary critical infrastructure. HHS plans to continue working with Healthcare and Public Health Sector, and Food and Agriculture Sector, stakeholders to raise awareness and encourage their participation in the workshops and the Framework's review process.

HHS and Civil Liberties:

HHS takes seriously its responsibility to analyze and mitigate the risks to privacy and civil liberties that could be implicated by any of its activities. OGC regularly participates in discussions related to the Department's EO 13636 efforts. In partnership with the Cybersecurity Working Group, OGC informs Department executives about applicable legal authorities and limitations for proposed activities during the establishment and program planning phases of its various projects.

As mentioned in last year's report, HHS is not engaged in activities that implicate an individual's civil liberties, such as those involved in law enforcement or national security. The Department has extremely narrow and limited authorities regarding the ability to arrest or hold individuals in a way that would deprive them of their civil liberties. The National Institutes of Health (NIH) does have a campus police force; and the FDA has law enforcement authority to protect FDA-regulated products. However, in the case of an incident, those agencies generally coordinate and cooperate with other law enforcement entities external to the Department, such as local law enforcement officials or the Federal Bureau of Investigation (FBI). As shown with the recent Ebola issue, the Centers for Disease Control and Prevention (CDC) has public health authority to order the apprehension, detention, including the isolation or quarantine, or conditional release, of individuals arriving into the United States from a foreign country, or moving between states, if it reasonably believes that such individuals are either infected with or were exposed to one of nine quarantinable diseases, as defined in Executive Order 13295, as amended. The CDC relies on other federal agencies, in particular Customs and Border Protection and the U.S. Coast Guard, or State and local entities, for their law enforcement assistance in carrying out its responsibilities when the individual in question is not compliant with public health orders. These legal authorities are rarely used, and, if exercised, only when necessary to determine whether a foreign traveler may have exposed other passengers travelers to a dangerous, communicable disease or, if necessary, to allow for a smooth transition to state or local public health control.

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 1974² 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:

The primary new HHS activity for the FY14 reporting period is the initiative to increase collaboration across HHS:

- Evaluation of whether or not any programs subject to EO 13636 have been overlooked;
- Maintaining awareness of any programs being developed or adapted that would make them a "critical infrastructure" program, under the definition provided in EO 13636; and
- Increasing engagement in external activities, such as the NIST Cybersecurity Framework.

As the volume of information and programs that HHS must review and account for, our collaboration and partnerships will be the key to HHS's success.

Conclusion:

In response to last year's report, PCLOB agreed with our conclusion that HHS did 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.

² 5 U.S.C. § 552.

PART VII: DEPARTMENT OF ENERGY



Introduction

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

Privacy and Civil Liberties Program

DOE has an appointed Chief Privacy Officer (CPO) who manages the department's privacy program to ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 U.S.C. 552a, Section 208 of the E-Government Act of 2002, and Office of Management and Budget privacy directives. The CPO advises DOE program elements on privacy matters associated with their operational missions.

Energy Sector: Smart Grid

The energy sector critical infrastructure has been subjected to a dramatic increase in focused cyber attacks in recent years. The sophistication and effectiveness of these intrusions marks the transition to an era of state actor level threats to the United States. As the energy sector-specific agency (SSA), DOE has the mission and domain expertise to work with industry to mitigate the risk resulting from the cyber-physical coupling within the energy environment. The long history of DOE collaboration with industry has created relationships that are integral to activities that expand situational awareness and information sharing to reduce cyber risk. Reliable and resilient energy infrastructure is essential to the economy, health and safety, and our national security. Cybersecurity for energy delivery systems has emerged as one of the Nation's most vital grid modernization and infrastructure security issues. Innovative solutions designed to meet the unique requirements of high-reliability energy delivery systems are urgently needed to ensure the success of grid modernization and transformation of the Nation's energy systems to meet future needs for economic growth. Effective solutions must be based on industry best practices, sound risk management processes, and improved situational awareness, and will require multi-disciplinary collaborations and shared expertise in power systems engineering, computer science, and cybersecurity.

The Smart Grid applies available technologies, tools and techniques to make the nation's electric system work more efficiently and to provide consumers with the ability to monitor and manage their electricity use by providing visibility and access to data generated by smart meters.

This assessment applies to DOE activities related to the implementation of the Smart Grid. DOE has instituted policies that address privacy protections to be applied to federal activities associated with personal information in connection with any departmental function.¹ As the nation's electric infrastructure is modernized, it is a priority to ensure that consumers' privacy is

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

protected while also encouraging and allowing for innovation for the greatest benefits for consumers.

These policies incorporate both statutory and regulatory privacy requirements with which DOE are required to comply and leverages best practices that DOE has determined are essential to provide adequate privacy and civil liberties protections to data collected as the Smart Grid evolves. 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, is working closely with all Smart Grid stakeholders to protect consumers' customer data which includes energy usage information.

As the energy SSA, the Department's ongoing collaboration with vendors, utility owners, and operators of the electricity and oil and natural gas sectors strengthens the cybersecurity of critical energy infrastructure against current and future threats. Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, directs the SSAs to serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities; carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and provide, support, or facilitate technical assistance and consultations for each sector to identify vulnerabilities and help prevent or mitigate the effects of incidents, as appropriate. In meeting this requirement for the Department, OE's Cybersecurity for Energy Delivery Systems (CEDS) program is supporting cyber risk and incident management activities with the four key objectives:

- Accelerating information sharing to enhance situational awareness;
- Expanding implementation of the Cybersecurity Capability Maturity Models and Risk Management Process;
- Exercising and refining the energy sector's cyber incident response capabilities; and
- Promoting energy sector cybersecurity workforce development.

In FY2014, the Cybersecurity Risk Information Sharing Program (CRISP) transitioned from a small DOE-funded pilot to a private-sector funded and managed program with the North American Electric Reliability Corporation's (NERC) decision to expand its Electricity Sector Information Sharing and Analysis Center duties to include the management of CRISP for the electricity subsector. 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.

The vast majority of actionable cyber threat information is unclassified and in the possession of the private sector. CRISP attempts to enrich this unclassified information with classified U.S. Government information and develop the necessary context and relevance to support energy sector decision making, while also improving the Government's situational awareness of the energy sector threats. This enrichment process is uniquely governmental and fills a critical gap in commercially available cyber threat information services.

The Master Agreement between NERC and the DOE National Laboratory performing the CRISP analysis includes a detailed Data Handling Guide that addresses all aspects of data handling, with specific emphasis on auditing, Department of Energy's (DOE) privacy oversight and sensitive data minimization.

While CRISP effectiveness is based on the sharing of information, it is important that the participants know and understand that they own their own data and may limit the dissemination and disposition of information from or about their site. Each participant also controls how it uses the information provided to them by the Government. At no point does a participant relinquish ownership of its data provided to CRISP. Each participant completes a data sharing matrix that describes the types of information that the participant is willing to share and with which other CRISP participants it is willing to share the information.

The full and successful implementation of CRISP as an enduring program will require industry and government to create a true public-private partnership that addresses and mitigates all sensitive legal and policy concerns on both sides of the partnership. Minimizing the role of government and leveraging the existing, significant capabilities of the private sector is the best way to address these valid concerns. Industry needs relevant and actionable information from the government to help protect its systems in an environment that is increasingly hostile. The government needs to better understand the threats faced by the industry every day to enable effective and timely sharing of actionable threat information, improve shared situational awareness, and facilitate jointly developed mitigation solutions.

Assessment Methodology

DOE has no jurisdiction to regulate or monitor either utilities or third parties who will be collecting or using the data provided/collected through smart grid technologies. Therefore, DOE in partnership with the Federal Smart Grid Task Force initiated a multi-stakeholder process to develop a Voluntary Code of Conduct (VCC) that would be legally enforceable through the FTC's jurisdiction as outlined in the administration's privacy blueprint².

For electric utilities, state regulators or utility boards have jurisdiction over privacy policies, but in many jurisdictions updated policies to address customer energy use data are just beginning to be investigated. The VCC while providing a public-facing method for communicating with consumers about privacy policies and, therefore, increasing consumer confidence, the VCC will also inform state commissions and utility boards as they develop their policies thus enabling more consistency across the US.

As DOE does not have jurisdiction as a regulatory body, a Voluntary Code that provides high-level concepts and principles related to data enabled through smart grid technologies and is legally enforceable through the FTC's jurisdiction was deemed to be the best method for pushing for advancements in privacy protections while not overstepping regulatory authorities. While adoption of the VCC is voluntary, once adopted by companies, it is legally enforceable through the Federal Trade Commission's authority over unfair and deceptive business practices.

² Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Privacy Blueprint).

Many policies exist to govern customers' personal information data such as date of birth, social security number, credit card information, etc.; however, with more granular information being collected through smart grid technologies and the addition of third parties interested in accessing this data to offer additional products and services, the VCC sought to leverage and expand those protections to the vast amounts of usage data made available through smart meters.

Stakeholders – leaders across the industry from utilities, regulatory staff, consumer advocates, and third-party providers – focused the VCC on five core concepts that were initially modeled on the categories outlined in the Fair Information Practice Principles (FIPPs). FIPPs are a widely accepted framework of privacy principles that provides the general basis for the Privacy Act of 1974, as amended and other privacy laws and policies.

E.O. 13636 Implementation Activities

DOE is the lead agency in coordinating the modernization of the nation's electric grid. DOE's Office of Electricity Delivery and Energy Reliability in concert with its research labs and policy programs, and the multi-agency Smart Grid Task Force coordinates standards development, directs research and development projects, and reconciles/coordinates the agendas of a wide range of stakeholders related to smart grid technology.

DOE recognizes that Smart Grid success depends upon respecting consumers' reasonable expectations of privacy, security, and control over who has access to energy-usage data. To that end, DOE is continuing efforts with affected stakeholders to protect customer privacy and to foster responsible data access to ensure consumers receive the maximum benefit from investments in Smart Grid technology.

Utilities will have access to energy consumption data for operational purposes (primary purposes³) and state utility commissions/utility boards have jurisdiction for regulating issues associated with data privacy. However, with smart grid technologies, utilities will have access to and may want to use customer energy use data (CEUD) for secondary (nonoperational) purposes. In addition, customers might want access to their own data or might want to authorize access to a third party for other products and services. The VCC describes principles to protect Customer Data while providing customers with appropriate access to their own Customer Data and not infringing on or superseding any law, regulation, or governance by any applicable federal, state, or local regulatory authority.

Privacy and Civil Liberties Assessment

As the nation's electric infrastructure is modernized, intelligence is being added to the grid throughout the U.S., through the deployment of advanced technology. These technologies with their increased intelligence present new opportunities and benefits for consumers and have introduced new entities wanting to offer new products and services. This has led to concerns regarding consumer data access and the privacy of consumer energy consumption data.

³ Definitions in the Voluntary Code of Conduct found at www.smartgrid.gov/privacy.

Historically, utilities have taken very seriously the job of protecting customers' privacy, and privacy and security protections will remain fundamental objectives. However, with the new technologies being deployed today and new, nonregulated entities entering the market, these fundamental protections warrant new attention. It is critically important that consumers feel secure that their data will be protected and treated responsibly. Much progress has been made toward this goal.

The VCC will be instrumental in providing utilities and third parties a mechanism for demonstrating how consumers' data is protected and secured. It will also provide public utility commissions and utility boards' baseline concepts and principles to use/reference as they modify and develop their specific regulations related to data collected through smart grid technologies thus helping to provide consistency across jurisdictions.

DOE OE concluded the multi-stakeholder effort to develop the VCC for utilities and third parties on protecting consumers' data, and the final VCC incorporates public comments received in response to the DOE Federal Register Notice, Volume 79, No. 177, September 12, 2014⁴.

The VCC structure, initially based on the FIPPs framework, is structured around the topics of Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security and Management/Redress. The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could adopt the VCC with some limited exceptions (such as when laws, regulatory guidance or frameworks, governing documents, policies, and/or consensus-driven state, local, or utility industry business practices require a different approach). Such exceptions, however, should be consistent with the overall purposes of the VCC and should be explicitly noted and explained in any depiction of VCC adoption, such as in a privacy policy or other notice. Nothing in the VCC is intended to change, modify, or supersede federal, state, or local laws or civil liberties protections. Specifically, no information shall be collected or maintained on how an individual exercises rights protected by the first amendment to the U.S. Constitution, including the freedoms of speech, assembly, press and religion. The following provides a summary of each section of the VCC:

- **Consumer Notice and Awareness** – Specifies how the customer learns what he or she needs to know to exercise informed choice. It describes requirements for practices that explain data collection policies and procedures to customers, focusing on customer options and responsibilities.
- **Customer Choice and Consent** – Specifies how the customer controls his or her data and under what limitations. It describes the requirements for processes that allow the customer to control access to his or her data for Secondary Purposes (i.e., to authorize differential access to multiple Third Parties, limit the duration of access, keep a record of data releases, rescind authorizations, and dispose or de-identify data once authorization or the need for the data has expired), identifies data types and disclosures that do not require customer consent, and includes a requirement requiring certain data to be obtained directly from the customer.

⁴ <http://energy.gov/oe/downloads/data-privacy-and-smart-grid-voluntary-code-conduct-notice-public-comment-federal>

- **Customer Data Access and Participation** – Specifies how the customer’s data is accessed. It describes requirements for procedures that allow customers to access their data, identify possible inaccuracies, and request they be corrected, and includes the potential for fees for non-standard requests.
- **Integrity and Security** – Specifies how customer data is maintained, and describes requirements for a cyber security risk management program, and methodologies for creating Aggregated or Anonymized Data.
- **Self-Enforcement Management and Redress** – Specifies how the VCC is followed. This section describes requirements for actions by Service Providers who voluntarily adopt the Voluntary Code of Conduct to ensure that compliance with it.

Recommendations

Through the multi-stakeholder process, DOE OE has conducted focus groups to gauge consumer sentiment and determine how consumers would like to be communicated about the VCC. Consumer reaction to the VCC has been highly positive and entities involved in the process are seeing the benefits it will provide. It will be critical to raise awareness of the VCC among consumers and adopting entities to ensure widespread adoption.

PART VIII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



**Office of the Director of National Intelligence
Civil Liberties and Privacy Office
February 13, 2015**

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). I lead the ODNI Civil Liberties and Privacy Office (CLPO). 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 31, 2014. Our initial assessment was submitted on December 2, 2013 for inclusion in the first Department of Homeland Security (DHS) Cyber Report, consistent with the mandate of EO 13636.

ODNI's activities under EO 13636 have not materially changed since our last assessment. This activity primarily involved the development and dissemination of guidance to the Intelligence Community for timely producing unclassified cyber products that identify a specific targeted entity. ODNI determined that Intelligence Community Directive (ICD) 209, Tearline Production and Dissemination, meets this requirement. ICD 209 was not modified in the current reporting period. As last year's submission included a comprehensive civil liberties and privacy assessment of that Directive, we did not repeat that analysis this year.

In writing our assessment last year, we were cognizant of the role assigned ODNI (i.e., review, comment, coordinate) with respect to the cyber activities that EO 13636 prescribed for DHS, the Department of Justice, and National Institute of Standards and Technology. At that time, those activities were in their infancy so the extent of our participation was not ripe for assessment. Those agencies' activities are now complete, and we understand that the lead agencies have been assessing those activities pursuant to their obligations under EO 13636. We do not believe that ODNI engagement at the coordination level warrants further assessment by this office.

Although our assessment last year found the tearline instruction is consistent with privacy and civil liberties protections, we recommended that training be developed related to the protection of individuals' privacy and civil liberties in tearline products. The ODNI CLPO has recently completed an online training module for intelligence personnel, specifically addressing the use and disclosure of personally identifiable information about US persons. This training module is applicable to the production and dissemination of tearlines and will be made available to the Intelligence Community; it therefore is responsive to our earlier recommendation. This module also may serve as the basis for training regarding protections (potentially affecting cyber tearline production) for non-US persons in certain contexts, as mandated by Presidential Policy Directive (PPD-28), Signals Intelligence Activities.

In addition, the Intelligence Community is engaged in a range of activities that may result in further protections for identifiable individuals. These protections also apply to cyber-related intelligence products.

- ODNI has initiatives in progress to review Intelligence Community policies to ensure that intelligence products containing personally identifiable information are corrected when they are subsequently determined to be inaccurate.
- The Intelligence Community and ODNI are implementing civil liberties and privacy protections for information obtained through Signals Intelligence, as required by PPD-28. It is likely that these measures will impact the privacy protection afforded subjects of tearlines covered by EO 13636.
- The ODNI National Intelligence Manager for Cyber is conducting an efficacy study of the use of ICD 209 to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. This study will help determine the need for revised or additional policy guidance.
- The President has directed the DNI to establish a Cyber Threat Intelligence Integration Center (CTIIC). To the extent that CTIIC is involved in activities covered by Section 4 of EO 13636, an assessment of those activities will be conducted as provided for in the EO.

Although it is premature to attempt an assessment in this period of the above initiatives, we are closely engaged on them, and will address them in subsequent assessments if applicable.

We note that as an organization ODNI has not issued any cyber tearlines covered by EO 13636. In the absence of tearline activity this period, no audit of ODNI tearline processes has been conducted. If ODNI were to issue such a tearline, ODNI/CLPO would provide guidance consistent with ICD 203, Analytic Standards, which provides that personally identifying information should be "included in products only as it relates to a specific analytic purpose (e.g., necessary to understand the foreign intelligence or counterintelligence information or assess its importance)." In that hypothetical situation the disseminated tearline would be disposed of in accordance with the applicable records control schedule established with the National Archives and Records Administration.

Sincerely,

[SIGNATURE ON FILE]

Alexander W. Joel
Civil Liberties Protection Officer