

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

November 2018





FOREWORD

November 2018

We are pleased to present the 2018 Executive Orders 13636 and 13691 Privacy and Civil Liberties Assessments Report. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience* issued on February 12, 2013, directed federal departments and agencies to work together and with the private sector to strengthen the security and resilience of the Nation's critical infrastructure. Specifically, Executive Order 13636 requires federal agencies to develop and incentivize participation in a technology-neutral cybersecurity framework, and to increase the volume, timeliness, and quality of the cyber threat information they share with the private sector.

Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, issued on February 13, 2015, acknowledges that organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. That Executive Order encourages the formation of such information sharing organizations, establishes mechanisms to improve their capabilities, and enables them to better partner with the Federal Government on a voluntary basis.

Section 5 of both Executive Orders requires that federal agencies coordinate with their respective senior agency privacy and civil liberties officials ("Senior Officials") to ensure that appropriate protections for privacy and civil liberties are incorporated into any activities conducted under the Orders. The Senior Officials are also required to annually assess and report upon the privacy and civil liberties impacts of their respective agencies' activities undertaken pursuant to each Executive Order. The Senior Officials must submit those assessments to the Department of Homeland Security (DHS) Office for Civil Rights and Civil Liberties and the DHS Privacy Office for inclusion in this Privacy and Civil Liberties Assessment report.

This fifth annual report provides assessments of activities conducted under Executive Orders 13636 and 13691 during fiscal year 2017. The scope of the report is limited to those activities with a privacy or civil liberties impact, which are new or substantially changed since the fiscal year 2016 reporting cycle.

Participating departments and agencies have varying levels of participation in implementing activities, and only DHS was engaged in activities conducted pursuant to Executive Order 13691. The chart below provides a brief overview of the activities assessed by the reporting Senior Officials.

2018 Executive Order 13636 / 13691 Section 5 Reports by Department and Topic

	DHS	DOD	DOJ	DOE	ODNI	Commerce	HHS	Treasury
E.O. 13636								
4(a) Cybersecurity Information Sharing			X		X			X
4(b) Dissemination of Cyber Threat Reports			X					
4(c) Enhanced Cybersecurity Services / Defense Industrial Base Program		X						
4(d) Private Sector Clearance Program								X
9(a) Critical Infrastructure Identification								X
Other				X				
Conducted Review But Nothing New or Significant to Report	X					X ¹	X	
E.O. 13691								
Conducted Review But Nothing New or Significant to Report	X							


¹ The Department of Commerce conducted an assessment of its activities under Executive Order 13636 and determined that a report was not required. In lieu of input for inclusion in this report, the Department of Commerce reported to our offices in writing that it had completed its assessment and would not be providing a report or letter in this reporting cycle.

In addition to conducting the DHS Privacy and Civil Liberties Assessment, our offices – the DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office – coordinated the interagency report compilation process with the Senior Officials for each reporting agency. In this capacity, our offices acted as process managers, leaving the other reporting Department and agency Senior Officials free to assess and report on activities at their respective agencies in an objective and independent manner, consistent with their own authorities, policies and judgment. We did not direct the Senior Officials in the selection of activities for assessment, their assessment methods, or in the drafting of their reports. The reporting Senior Officials did, however, work jointly with our offices to produce this report, sharing best practices, following similar formats, and coordinating assessment coverage for those sections of Executive Order 13636 that are implemented simultaneously in multiple agencies.

Each agency’s report reflects its own Senior Officials’ determination regarding which activities required assessment and reporting under Executive Orders 13636 and 13691, or were otherwise deemed appropriate to be assessed.

Our offices also facilitated communications between the Senior Officials and the United States Privacy and Civil Liberties Oversight Board (“the Board”) acting in its consultative role, as specifically required by Section 5 of Executive Order 13636. Each Senior Official worked independently and directly with the Board without DHS involvement, to maximize the Senior Officials’ latitude for disclosure and responsiveness to the Board.

To view past years’ privacy and civil liberties assessments conducted under Executive Order 13636, please visit: <https://www.dhs.gov/cybersecurity-and-privacy>.



Cameron P. Quinn
Officer for Civil Rights and Civil Liberties



Phillip S. Kaplan
Chief Privacy Officer

TABLE OF CONTENTS

FOREWORD.....	2
PART I: DEPARTMENT OF HOMELAND SECURITY.....	6
PART II: DEPARTMENT OF THE TREASURY.....	14
PART III: DEPARTMENT OF DEFENSE.....	17
PART IV: DEPARTMENT OF JUSTICE.....	20
PART V: DEPARTMENT OF HEALTH AND HUMAN SERVICES.....	24
PART VI: DEPARTMENT OF ENERGY.....	27
PART VII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.....	31

PART I: DEPARTMENT OF HOMELAND SECURITY



I. Introduction

Background and Scope

Section 5 of Executive Orders 13636 and 13691 require that the DHS Chief Privacy Officer and DHS Officer for Civil Rights and Civil Liberties assess the privacy and civil liberties risks of the functions and programs the Department of Homeland Security (DHS or Department) undertakes pursuant to these Executive Orders. This assessment, together with any recommendations for minimizing or mitigating identified risks, is included in an annual public report. In addition, the DHS Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) coordinate and compile in a single published report the Privacy and Civil Liberties assessment reports conducted by the senior officials for privacy and civil liberties from other Executive Branch departments and agencies that have reporting responsibilities under these Executive Orders.

As in previous Executive Order 13636 assessments, the scope of this year's assessment is limited to new DHS activities that were undertaken during the past Fiscal Year as a result of Executive Orders 13636 and 13691, or those pre-existing DHS activities that were substantially altered by these orders during the past Fiscal Year. The review of Department activities in this reporting cycle included all activities conducted by DHS under Executive Orders 13636 and 13691 during fiscal year 2017. After a thorough review, the DHS Privacy Office and CRCL concluded that there were no new DHS activities undertaken during Fiscal Year 2017 as a result of Executive Orders 13636 or 13691, nor were there any pre-existing Executive Order 13636 or 13691-related DHS activities that were substantially altered during Fiscal Year 2017.

Section 5 of both Executive Orders 13636 and 13691 directs the assessment of the “functions, programs, and activities undertaken by DHS under the Orders,” and the scope of the assessment is therefore limited to those functions and programs, and does not assess the many cybersecurity programs and activities conducted by DHS under other authorities. 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).² The mission of the Privacy Office is to protect individual privacy 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.

² 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 the interagency community;
- 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.³

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 Civil Rights and Civil Liberties reports directly to the Secretary of Homeland Security. CRCL integrates civil rights and civil liberties into all of the Department'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.⁴

³ Detailed information about DHS Privacy Office activities and responsibilities, including Privacy Impact Assessments published by the Privacy Office for DHS cybersecurity-related efforts, is available at <http://www.dhs.gov/privacy>.

⁴ See 6 U.S.C. § 345. Detailed information about the activities and responsibilities of the DHS CRCL is available at <http://www.dhs.gov/office-civil-rights-and-civil-liberties>.

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

Executive Order 13636 and Executive Order 13691 direct the senior officials for privacy and civil liberties of agencies engaged in activities under the orders to perform an “evaluation of activities against the Fair Information Practice Principles (FIPPs) and other applicable privacy and civil liberties policies, principles, and frameworks.”⁵ DHS has evaluated its activities against the FIPPs and other applicable privacy and civil liberties policies, principles, and frameworks. More information on the evaluation process is described below.

The DHS Privacy Framework

The FIPPs, which are rooted in the tenets of the Privacy Act of 1974,⁶ have served as DHS’s core privacy framework since the Department was established. They are memorialized in the DHS Privacy Office Privacy Policy Guidance Memorandum 2008-01, “The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security” (December 29, 2008)⁷ and in DHS Directive 047-01, “Privacy Policy and Compliance” (July 7, 2011).⁸ 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 of records using PII must be described in a System of Records Notice (SORN)⁹ and Privacy Impact Assessment (PIA),¹⁰ as appropriate. With

⁵ Section 5(a), E.O. 13636.

⁶ 5 U.S.C. § 552a.

⁷ Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

⁸ Directive 047-01 is available at <http://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf>. The Directive supersedes DHS Directive 0470.2, Privacy Act Compliance, which was issued in October 2005.

⁹ The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding personally identifiable information (PII) collected and retrieved by a personal identifier 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 describe 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.

¹⁰ The E-Government Act of 2002 (44 U.S.C. § 3501) and the Homeland Security Act (6 U.S.C. § 142(a)(4)) establish the requirements for publishing 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 information technology (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.

the exception of a small number of PIAs for national security systems, there should be no system the existence of which is a secret.

Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Purpose Specification: DHS should specifically articulate the authority that 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 (NARA).

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 media) 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 privacy-related policies and activities at DHS. DHS uses the FIPPs to assess privacy risks and enhance privacy protections by assessing the nature and purpose of all PII collected to ensure it is necessary for the Department's mission to preserve, protect, and secure the homeland. The DHS Privacy Office applies the FIPPs to the full breadth and diversity of Department systems, programs, and initiatives that use PII, or are otherwise privacy-sensitive, including the Department's cybersecurity-related activities. Because the FIPPs serve as the foundation of privacy policy at DHS, the Privacy Office works with Department personnel to complete Privacy Threshold Analyses (PTA), PIAs, and SORNs to ensure the implementation of the FIPPs at

DHS.¹¹ When conducting a Privacy Compliance Review (PCR)¹², the Privacy Office evaluates the program’s compliance with the FIPPs, any requirements outlined in its PTA, PIA, or SORN, and any privacy policies that are specific to that program. It is important to note, however, that because DHS uses the FIPPs as its foundational privacy policy framework, many DHS programs or activities do not require specific privacy policies aside from DHS’s Privacy Policy Guidance Memorandum on the FIPPs, DHS Directive 047-01 “Privacy Policy and Compliance,” and any specific privacy requirements documented in an applicable PTA, PIA, and/or SORN.

Civil Rights and Civil Liberties Assessment Framework

CRCL conducts assessments using an issue-spotting approach rather than a fixed template of issues because the particular issues that may be presented vary greatly across programs and activities. This approach necessitates an 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, authority or policy that may be relevant in specific instances, such as treaty obligations to which the United States has consented establishing 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 issues affecting individual rights 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 (OGC) as

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

¹² The 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.

appropriate, to craft workable policy recommendations and solutions to ensure individual rights are appropriately protected within the assessed program or activity. These solutions may be embedded in program-specific policies, operating procedures, other documentation or simple changes in program activities, as appropriate.

Related DHS Privacy and Civil Liberties Cyber Activities

Our work under Executive Orders 13636 and 13691 provides further transparency into the Department's cybersecurity-related activities dating back to PIAs and SORNs first published in 2004 and updated since that time.¹³ In addition, the Department has sought the guidance of its Data Privacy and Integrity Advisory Committee (DPIAC)¹⁴ 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.

II. Executive Orders 13636 and 13691

In this year's report, as noted, the DHS Privacy Office and CRCL concluded that there were no new DHS activities undertaken during fiscal year 2017 as a result of Executive Orders 13636 or 13691, nor were there any pre-existing Executive Order 13636 or 13691-related DHS activities that were substantially altered during the past Fiscal Year. DHS, however, continues to conduct the programs and activities directed by Executive Order 13636, which have been reported upon and assessed in prior Executive Order 13636 Privacy and Civil Liberties Assessment Reports.

Additionally, the Information Sharing and Analysis Organizations (ISAO) Standards Organization, established by Section 3(a) of Executive Order 13691 and selected by DHS in 2015, has continued its work with existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders to identify a common set of voluntary standards or guidelines for the creation and function of ISAOs.¹⁵ As in prior Assessment Reports, DHS is not undertaking a detailed analysis of the Standards Organization's published ISAO guidelines or ISAO implementation because the Standards Organization's work is not an activity of the Department within the meaning of Section 5 of Executive Order 13691.¹⁶

¹³ These PIAs and links to associated SORNs are available on the DHS Privacy Office's website, in the domain covering the Department's National Protection and Programs Directorate (NPPD) at <http://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd>.

¹⁴ 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>.

¹⁵ More information about the Standards Organization, the process by which the standards were developed, and the actual standards themselves are available at the Standards Organization's website, <https://www.isao.org/>.

¹⁶ The discussion of the policies of the ISAO Standards Organization in last year's report was beyond the scope of the assessment required by Executive Orders 13636 and 13691. That information was provided because the Office for Civil Rights and Civil Liberties and the DHS Privacy Office periodically include information in this annual report in excess of the requirements of Section 5 of the Executive Orders for transparency purposes.

In addition, as detailed in the 2017 Executive Order 13636 Privacy and Civil Liberties Assessment Report, DHS continues to engage in continuous, collaborative, and inclusive coordination with ISAOs via the DHS National Cybersecurity and Communications Integration Center (NCCIC), which coordinates cybersecurity information and analysis amongst the Federal Government and private sector partners through two main programs: the Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) Initiative. These sharing mechanisms were not substantially altered in Fiscal Year 2017, thus, DHS has nothing significant to report in this year's Assessment Report.

As the Department continues its implementation activities under these two Executive Orders, the DHS Privacy Office and CRCL will assess new activities, and provide any necessary updates to previous assessments in future reports.

PART II: DEPARTMENT OF THE TREASURY





DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

February 13, 2018

Ms. Cameron Quinn
Officer for Civil Rights and Civil Liberties
Department of Homeland Security
Office for Civil Rights and Civil Liberties
245 Murray Lane, SW
Building 410, Mailstop 190
Washington, DC 20528-0190

Mr. Sam Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
245 Murray Lane, SW
Mailstop 0655
Washington, DC 20528

Subject: Department of the Treasury Privacy and Civil Liberties Assessment

Dear Ms. Quinn and Mr. Kaplan:

On behalf of the Department of Treasury Senior Agency Official for Privacy (SAOP) and Chief Privacy and Civil Liberties Officer, I am pleased to submit a summary of Treasury's activities this year under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. In accordance with Section 5(b) of the EO, this letter constitutes my assessment of the Department of the Treasury's activities carried out under the EO for the October 1, 2016 to September 30, 2017 reporting period.

Treasury reviewed its 2016 report and determined that its activities under the EO have not materially changed since we last reported. Because our activities have not substantively changed from those reported in 2016, revisions to the previously filed report are not necessary and we have not included a privacy and civil liberties assessment with this letter. Instead, we are providing a summary of our activities under the EO and rely upon our previous disclosures in the 2016 report.

Treasury continues to play a minor role in disseminating PII in two programs: Information Sharing under section 4(a) of the EO, and the Critical Infrastructure Private Sector Clearance Program under section 4(d) of the EO. In addition, Treasury continues to play a minor role in identifying critical infrastructure where a cybersecurity incident could reasonably result in catastrophic consequences ("high risk critical infrastructure"), as required under section 9(a) of the EO.

As the Sector-Specific Agency for the Financial Services Sector, Treasury continues to receive requests for nominations for national security clearances to allow financial services critical infrastructure owners, operators, and sector leaders to access cyber threat information. Through a consultative process developed under EO 13636, Treasury continues to assist law enforcement and national security agencies with identifying high risk critical infrastructure.

As discussed more fully in the 2016 report, Treasury also continues to identify 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 and other critical infrastructure partners for use in network defense. This information consists of malicious cyber actors' tactics, techniques, procedures (TTPs) and associated indicators, to assist in network defense capabilities and planning. Treasury occasionally receives cyber threat information on malicious cyber actors' TTPs and associated indicators from the financial services sector and continued to do so during the current reporting period.

In this reporting period, Treasury appropriately shared cyber threat information with the financial services sector in the form of unclassified Cyber Information Group (CIG)¹⁷ Circulars, through monthly meetings, and upon request from the financial services sector or a member of the sector. In the 2016 report, we discussed the future development of a retention schedule for the information contained in CIG Circulars. Treasury's Office of Privacy, Transparency, and Records (PTR) received guidance from the National Archives Records Administration (NARA) regarding the current existence or creation of a retention schedule for the cyber information shared in CIG Circulars. PTR will continue to work with NARA and expects completion of the schedule during the 2019 fiscal year.

Treasury continues to play a minor role in the dissemination of PII for the programs described above. In the future, Treasury plans to continue its work to assist in the dissemination of cybersecurity information while protecting privacy and civil liberties. If Treasury's role expands or the Department substantially changes its activities under the order, we will provide a comprehensive updated privacy and civil liberties assessment of those activities in future reports.

Sincerely,

Ryan Law
Deputy Assistant Secretary
for Privacy, Transparency, and Records
U.S. Department of the Treasury

¹⁷ The CIG consists of a specialized team of analysts with expertise in financial services, cybersecurity, and intelligence analysis. The CIG's primary function is to distribute timely and actionable information and analysis that financial institutions can use to protect themselves from cyber attacks.

PART III: DEPARTMENT OF DEFENSE



Ms. Cameron Quinn
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, D.C. 20528

September 6, 2018

Dear Ms. Quinn:

I write as the Department of Defense (DoD) Privacy and Civil Liberties Officer to provide an update of the Department's privacy and civil liberties review of its critical infrastructure cybersecurity information sharing activities during Fiscal Year (FY) 2017, October 1, 2016 through September 30, 2017. DoD submits this letter as its part of the Department of Homeland Security's (DHS) report in accordance with Executive Order (E.O.) 13636, "Improving Critical Infrastructure Cybersecurity"¹⁸ and Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience."¹⁹

The Department primarily engages in critical infrastructure cybersecurity information sharing through the DoD Defense Industrial Base (DIB) Cybersecurity (CS) Program. In the Department's previous submissions to the DHS's reports, DoD provided a full privacy and civil liberties assessment and updates of those assessments, based on the Fair Information Practice Principles, of the DIB CS Program. During this reporting period, the critical infrastructure cybersecurity information sharing activities under the DIB CS Program did not substantially change from those analyzed under prior privacy and civil liberties assessments; however, a few updates are worth noting.

Industry participation in the DIB CS Program expanded to 255 companies – a 37 percent increase from FY 2016, with participating companies representing \$255B in defense revenue. Expanded outreach efforts to companies eligible to join the DIB CS Program through exhibits and briefings at government procurement and industry association meetings helped influence the participation increase. Senior DoD leadership engagements with the defense industry and participating DIB companies' encouragement to other companies and their suppliers to join the program also bolstered participation.

To safeguard the information shared within the expanding DIB CS Program, each participating company signs an agreement that incorporates the provisions of 32 Code of Federal Regulations (CFR) part 236²⁰ establishing a comprehensive approach for enhancing and supplementing DIB information assurance capabilities and conducting activities in accordance with applicable laws and regulations. Under this agreement, each party also ensures the confidentiality of information exchanged will be protected to the maximum extent authorized by law, regulation, and policy.

¹⁸ Available at <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

¹⁹ Available at <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

²⁰ Available at <https://www.gpo.gov/fdsys/pkg/CFR-2013-title32-vol2/pdf/CFR-2013-title32-vol2-part236.pdf>.

Further, the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012²¹ mandates cyber incident reporting by defense contractors and those companies providing operationally critical support. In accordance with this DFARS Clause, defense contractors are required to report compromises of their unclassified networks or information systems to a single web portal using the same process for mandatory and voluntary reporting, while also ensuring that privacy and civil liberties protections continue to be effective.

As reported in last year's submission, DoD updated its main privacy and civil liberties compliance documentation covering the DIB CS Program, including the Privacy Impact Assessment titled "Defense Industrial Base (DIB) Cybersecurity Activities" and the system of records notice titled "Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records." In addition, DoD submitted updates to information collection requests for cyber incident reporting and cloud computing, DIB CS Program cyber incident reporting, and the application process for joining the DIB CS Program. During this reporting period, DoD continued to monitor the DIB CS Program to ensure that the program was compliant with applicable federal privacy and civil liberties laws and requirements and that associated compliance documentation remained accurate and up-to-date.

In addition to the DIB CS Program, the DoD continues to participate in the Automated Indicator Sharing (AIS) Initiative, which is a DHS program enabling the timely exchange of cyber threat indicators and defensive measures between public and privacy entities. AIS participants must agree to terms-of-use²² requiring that indicators and defensive measures are used for cybersecurity purposes in accordance with these Terms, applicable law, and any handling requirements specified by the DHS. Detailed privacy and civil liberties assessments of the AIS Initiative can be found in DHS's PIA²³ and in its submission to this report.

DoD will continue to adhere to Federal law and DoD policies to protect individual privacy and civil liberties when it participates in programs to collect and share cybersecurity threat information. As programs and activities in this area change, DoD will provide further updates to DHS on any privacy and civil liberties assessments and reviews conducted in support of the government's efforts to secure our nation's critical infrastructure.

John H. Gibson II

cc:

Mr. Philip S. Kaplan
Chief Privacy Officer

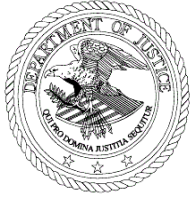
²¹ Available at <https://www.gpo.gov/fdsys/pkg/FR-2016-10-21/pdf/2016-25315.pdf>.

²² Available at https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf.

²³ See DHS/NPPD/PIA-029(a), Automated Indicator Sharing (AIS) at https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_ais_update_03162016.pdf.

PART IV: DEPARTMENT OF JUSTICE





U.S. Department of Justice

Office of the Deputy Attorney General

Telephone: (202) 514-0208

Washington, D.C. 20530

November 13, 2018

Ms. Cameron Quinn
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, DC 20528

Mr. Phillip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, DC 20528

Dear Ms. Quinn and Mr. Kaplan:

As the Acting Chief Privacy and Civil Liberties Officer (“CPCLO”) of the U.S. Department of Justice (“DOJ” or “the Department”), I am the designated senior agency privacy and civil liberties official responsible for providing the two of you with the Department’s annual privacy and civil liberties assessment on the Department’s critical infrastructure cybersecurity information sharing activities, pursuant to Section 5(b) of Executive Order (“EO”) 13636, Improving Critical Infrastructure Cybersecurity (February 12, 2013). As I explain below, the Department’s critical infrastructure information sharing activities have not substantially changed during the reporting period, making the format of a letter the best way to update you about our activities in this area.

As you are aware, EO 13636 directs the U.S. 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. Section 5 of EO 13636 directs both of you, as the Chief Privacy Officer (“CPO”) and the Officer for Civil Rights and Civil Liberties (“OCRCL”) of the Department of Homeland Security (“DHS”), on an annual basis, to jointly assess the privacy and civil liberties implications of the cybersecurity information sharing

activities of DHS and the other agencies named in EO 13636. EO 13636 then directs you to make recommendations to the DHS Secretary of ways to minimize or mitigate such risks in a publicly available report. EO 13636 establishes a process in which senior agency privacy and civil liberties officials for the other federal agencies engaged in cybersecurity information sharing activities under EO 13636 are to conduct their own privacy and civil liberties assessments. They are then to send you a report of their assessments for consideration and inclusion in the government-wide EO 13636 Privacy and Civil Liberties Assessment Report for which you are responsible.

Since its inaugural EO 13636 Privacy and Civil Liberties Assessment Report in 2014, the Department has annually reviewed its privacy and civil liberties assessment, and revised its report of that assessment, as necessary. The Department's assessment includes a description of the Department's privacy and civil liberties framework, as well as the Department's cybersecurity framework. The Department engages in cybersecurity information sharing under EO 13636 through activities undertaken by the Federal Bureau of Investigation ("FBI"). Accordingly, the Department's assessment reports included descriptions of FBI-specific frameworks and protections for privacy and civil liberties.

As I mentioned above, after conducting the annual review, I have determined that DOJ's activities under EO 13636 have not substantially changed since the Department's last assessment report, which addressed the reporting period of Fiscal Year 2016 and provided current information through July 2017.²⁴ As such, there is little new to report. This letter, however, updates and clarifies the Department's on-going role in implementing certain provisions of EO 13636, addressing the period since our last assessment report.

For the instant government-wide assessment report, the Department participated in an interagency working group to coordinate the report's review and revision. This working group is led by representatives from DHS, in collaboration with the White House's National Security Council. Through these working group discussions and meetings, the Department has also consulted with the Privacy and Civil Liberties Oversight Board.

I. Implementation of Section 4(a)

Section 4(a) of EO 13636 establishes as the policy of the U.S. Government a general requirement for agencies to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Section 4(a) also requires the DHS Secretary, the Attorney General ("AG"), and the Director of National Intelligence ("DNI") to issue instructions to ensure the timely production of unclassified cyber threats to the U.S. homeland that identify a specific targeted entity ("cyber threat reports"). As noted, the Department's activities under Section 4(a) have not substantially changed from those analyzed in its prior privacy and civil liberties

²⁴ The Department's 2017 EO 13636 Privacy and Civil Liberties Assessment Report is located at: https://www.dhs.gov/sites/default/files/publications/2017%20EO%2013636_13691%20Section%205%20Report_Signed%20012618_Final.pdf.

assessment reports.²⁵

II. Implementation of Section 4(b)

Under Section 4(b) of EO 13636, the DHS Secretary and the AG, in coordination with the DNI, are required to establish a process that rapidly disseminates cyber threat reports to a targeted entity. Such a process shall also include the dissemination of classified reports to critical infrastructure entities authorized to receive them, consistent with the need to protect national security information. Finally, Section 4(b) of EO 13636 requires the DHS Secretary and the AG, in coordination with the DNI, to establish a system to track the production, dissemination, and disposition of these reports, the so-called “4(b) solution.” While the Department’s activities under Section 4(b) have not substantially changed from those analyzed in our prior assessments, the FBI’s Information and Technology Branch continues to develop and enhance the current Cyber Guardian platform so that it can fully support the updated Joint Requirements Team Support Capability Requirements. During the last reporting period, the National Cyber Investigative Joint Task Force and the FBI had anticipated that these updated requirements would be fully integrated by the second quarter of Fiscal Year 2018. However, this target date has been delayed and is now expected to be completed in the last quarter of Fiscal Year 2018.

In conclusion, 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 DOJ’s activities as it implements its responsibilities under EO 13636 to inform targeted entities of the current cyber threat landscape facing them, not only today, but in the future.

Sincerely,

Peter A. Winn
Chief Privacy and Civil Liberties Officer (Acting)

²⁵ As noted in the Department’s prior privacy and civil liberties assessment reports, the Office of the Deputy Attorney General issued a Department Order requiring the timely production of unclassified cyber threat reports. *See* DOJ Order 3393-2013, Issuing Instructions Pursuant to Executive Order 13636 Regarding the Timely Production of Unclassified Reports of Cyber Threat Information (2013). The Order also requires that all actions taken pursuant to the Order must be consistent with the need to protect privacy and civil liberties.

PART V: DEPARTMENT OF HEALTH AND HUMAN SERVICES





June 26, 2018

Mr. Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
Washington D.C. 20528

Ms. Cameron Quinn
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington D.C. 20528

Dear Mr. Kaplan and Ms. Quinn,

Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, 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. EO 13636 § 5(c) requires the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the U.S. 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 U.S. 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 coordinating their activities with senior agency officials for privacy and civil liberties and ensuring that privacy and civil liberties protections are incorporated into activities, which are aimed at improving the security and resilience of physical and cyber critical infrastructure.

Pursuant to the requirements of EO 13636, this letter 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 for the period ending September 30, 2017. The Department’s previous assessments were submitted for inclusion in the DHS Cyber Reports for fiscal year (FY) 2014, FY 2015 and FY2016, consistent with the mandate of EO 13636. The Department’s activities under EO 13636 have not changed since our last assessment and we have determined there are no “net new” activities at our agency conducted under EO 13636 which would merit reporting.

HHS will continue to initiate and promote increased collaboration across the Department. Additionally, HHS will continue to evaluate whether or not any programs subject to EO 13636 have been overlooked; maintain awareness of any programs being developed or adapted that would make them a “critical infrastructure” program, under the definition provided in EO 13636; and increase engagement in external activities.

Sincerely

/s/

Beth Anne Killoran
Deputy Assistant Secretary for Information Technology
and Chief Information Officer

PART VI: DEPARTMENT OF ENERGY



U.S. DEPARTMENT OF ENERGY

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

Pursuant to the requirements of Executive Order (E.O.) 13636, *Improving Critical Infrastructure Cybersecurity* (2013), this update reviews the Department of Energy's (DOE) privacy and civil liberties activities under Section 5 of the E.O. for the fiscal year ending September 30, 2017. This report also includes recent developments in activities originally initiated during the 2017 reporting timeframe. A complete summary of these ongoing developments will be included in next year's report.

DOE is the sector-specific agency for the Energy Sector, which includes the Smart Grid. DOE's previous assessment was included in the consolidated 2016 Department of Homeland Security *E.O. 13636 Privacy and Civil Liberties Assessment*, consistent with the mandate of the E.O.

DOE's Office of Electricity (OE) and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) work in conjunction with various task forces and industry partners to provide transparency into efforts across private-sector and industry partners, including the protection of customer data. However, DOE itself lacks jurisdiction to regulate or monitor utilities or third-party entities that collect or use energy consumer usage data.

Previously, DOE reported on the efforts of the [DataGuard|Energy Data Privacy Program](#) (DataGuard) to secure a certification trademark through the U.S. Patent and Trademark Office (USPTO). The purpose of the trademark is to protect the DataGuard mark so that participating companies and entities can use the branding for their websites and products regarding the protection of consumer personal data. On April 4, 2017, the USPTO issued a Notice of Allowance for the trademark; however, the application remains under consideration by the USPTO.

Recent efforts include the launch of a DataGuard partnership program that offers member-based organizations a formalized way to indicate their support for the DataGuard concepts and principles. The DataGuard Energy Data Partnership Program was announced in June 2018 with the Smart Energy Consumer Collaborative (SECC) and the Green Button Alliance (GBA) as the first two inaugural members.

In May 2018, OE released the DOE *Multiyear Plan for Energy Sector Cybersecurity* (Plan) to improve cybersecurity and the resilience of the Nation's energy system. The Plan recognizes the

challenge of protecting sensitive operational information, including identifiable information about individuals during real-time threat monitoring and analysis data exchanges. The DOE Chief Privacy Officer is engaged with OE and CESER leadership to ensure that strong protections for the privacy and security of energy consumers are integrated into CESER's efforts, including working with CESER to adopt the joint Department of Homeland Security and Department of Justice *Privacy and Civil Liberties Final Guidelines* under the Cybersecurity Information Sharing Act of 2015.

CESER's Infrastructure Security and Energy Restoration (ISER) Division coordinates a national effort to secure U.S. energy infrastructure against all hazards, reduce impacts from disruptive events, and assist industry with restoration activities. ISER works closely with the electricity and oil and natural gas industries, other Federal agencies, and state, local, tribal, and territorial communities to advance national energy security and prepare for, respond to, and recover from evolving threats.

CESER's Cybersecurity for Energy Delivery Systems (CEDS) Division advances the research and development of innovative technologies, tools, and techniques to reduce risks to the Nation's critical energy infrastructure posed by cyber and other emerging threats. CESER's cybersecurity program supports activities in three key areas:

- Strengthening energy sector cybersecurity preparedness;
- Coordinating cyber incident response and recovery; and
- Accelerating research, development and demonstration (RD&D) of game-changing and resilient energy delivery systems.

Approximately 90 percent of the Nation's power infrastructure is privately held, meaning that coordination and alignment of information sharing between the government and the private sector is vital to safeguarding the Nation's energy sector. To achieve its vision, CESER works closely with representatives of the energy sector, companies that manufacture energy technologies, the National Laboratories, universities, other government agencies, and other stakeholders. CEDS activities include the ongoing support of RD&D of advanced cybersecurity solutions; the acceleration of information sharing to enhance situational awareness; and providing technical assistance to support the development and adoption of cybersecurity best practices.

CEDS is currently conducting Cybersecurity for the Operational Technology (OT) Environment (CYOTE) – OT Pilots. These Pilots will explore methods for enhanced bi-directional data sharing and analysis within the complex OT environment, where utilities currently have less mature tools for threat-detection during data collection and sharing activities on OT networks. The results from these Pilots will inform the development of a repeatable, standard approach that

the energy industry can use for real-time operational threat data sharing and analysis, including continuing improvements in monitoring, the collection and processing of threat data, and the safeguarding and protection of sensitive data and consumer privacy. CEDS will develop a Privacy Impact Assessment (PIA) for the Pilots.

Additionally, CEDS manages DOE's ongoing participation in the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a collaboration between the Federal Government and energy sector industry organizations to enable the timely, bi-directional sharing of threat information. CRISP also develops and deploys situational awareness tools to enhance the abilities of energy sector participants to identify threats and coordinate the protection of critical infrastructure.

The CRISP program completed its original PIA in November 2012. Since 2012, CRISP has added new participants and refined its analytical process, and has committed to conduct a new PIA for the program in FY2019.

Additional background information and guidance documents on these initiatives can be found on the following websites:

- Federal Smart Grid Task Force website:
<https://energy.gov/oe/technology-development/smart-grid/federal-smart-grid-task-force>
- DataGuard|Energy Data Privacy Program website:
<https://www.dataguardprivacyprogram.org/>
- Office of Cybersecurity, Energy Security and Emergency Response (CESER)
<https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response>
- *DOE Multiyear Plan for Energy Cybersecurity*, May 2018
https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

PART VII: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE INTELLIGENCE



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

December 5, 2017

Mr. Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
Washington, D.C. 20528

Ms. Cameron Quinn
Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Kaplan and Ms. Quinn:

I write as the Civil Liberties Protection Officer and the senior agency official for privacy and civil liberties of the Office of the Director of National Intelligence (ODNI). Pursuant to the requirements of Section 5(b) of Executive Order (EO) 13636 (February 12, 2013), Improving Critical Infrastructure Cybersecurity, this letter constitutes my review of ODNI's cyber activities for the period ending September 30, 2017.

This is our fifth review under EO 13636. Our fourth assessment was submitted on December 2, 2016, covering the period ending September 30, 2016, for inclusion in the fourth DHS Cyber Report. As indicated in prior submissions, our review covers the activities of the Cyber Threat Intelligence Integration Center (CTIIC), which provides integrated analytic products to other government agencies. The CTIIC Civil Liberties and Privacy Officer continues to provide civil liberties and privacy guidance to CTIIC personnel on the rules for disseminating information that contains information identifying or concerning a U.S. person (USPI).

As previously indicated in our submissions, CTIIC is not involved in U.S. private sector engagement covered by EO 13636 and therefore does not issue products that implicate the requirements of ICD 209, "Tearline Production and Dissemination." Should CTIIC ever become directly involved with cyber tearline reporting, my office will provide CTIIC with guidance and training consistent with ICD 203, "Analytic Standards" (regarding inclusion of personally identifiable information in analytic products), with ICD 209, with PPD 28 (if applicable), and with the rules regarding dissemination of USPI.

Sincerely,

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