



Executive Orders 13636 and 13691

Privacy and Civil Liberties Assessment Report

Compiled by:

The U.S. Department of Homeland Security Privacy Office and the
Office for Civil Rights and Civil Liberties

January 26, 2018



**Homeland
Security**



Foreword

January 26, 2018

We are pleased to present the 2017 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 fourth annual report provides assessments of activities conducted under Executive Orders 13636 and 13691 during fiscal year 2016. The scope of the report is limited to those activities with a privacy or civil liberties impact that are new or substantially changed since the end of fiscal year 2015.

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.

2017 Executive Order 13636 / 13691 Section 5 Reports by Department and Topic

	DHS	DoD	DOJ	ODNI	DOE	HHS	Treasury	Commerce
E.O. 13636								
4(a) Cybersecurity Information Sharing			X	X				
4(b) Dissemination of Cyber Threat Reports			X					
4(c) Enhanced Cybersecurity Services / Defense Industrial Base Program		X						
Other		X			X			
Conducted Review But Nothing New or Significant to Report						X	X	X ¹
E.O. 13691								
2(c) ISAO Information Sharing	X							
3(a) ISAO Standards Organization & Standards	X							

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 agency officials for each reporting agency. In this capacity, our offices acted as process managers, leaving the other reporting Department and agency senior agency officials free to assess and report on activities at their respective agencies in an objective and independent manner, consistent with their own

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.

authorities, policies and judgment. We did not direct the senior agency officials in their selection of activities for assessment, their assessment methods, or in the drafting of their reports. The

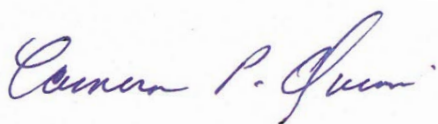
reporting senior agency officials did, however, work jointly with our offices to produce this report, sharing best practices, following similar formats, and coordinating assessment coverage for those sections of Executive Order 13636 that are implemented simultaneously in multiple agencies.

Each agency's report reflects its own senior agency 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 agency official worked independently and directly with the Board without DHS involvement, to maximize the senior agency officials' latitude for disclosure and responsiveness to the Board.

Because this year's report would ordinarily have been released during the Presidential transition period, final clearance of the report was suspended until politically accountable leadership at the reporting departments and agencies had an opportunity to review the report. Readers may note that that some reports contained herein contain references to senior privacy and civil liberties officials who are no longer serving with the current Administration, or to interim Senior Officials for Civil Rights and Civil Liberties at some agencies. This does not reflect any underlying errors, but accurately represents the identity of those who were serving in those positions when their contribution to this report completed clearance at their respective departments or agencies.

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



Philip S. Kaplan
Chief Privacy Officer

Contents

Foreword.....	2
Part I: U.S. Department of Homeland Security	6
Part II: U.S. Department of Defense	26
Part III: U.S. Department of Justice	31
Part IV: Office of the Director of National Intelligence	38
Part V: U.S. Department of Energy	41
Part VI: U.S. Department of Health and Human Services	44
Part VII: U.S. Department of the Treasury	47

Part I: U.S. Department of Homeland Security



I. Introduction

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

The review of Department activities in this reporting cycle included all activities conducted by DHS under Executive Orders 13636 and 13691 during fiscal year 2016. This year's report provides an assessment of DHS's fiscal year 2016 activities conducted under Section 2(c) of Executive Order 13691, and an update on activities conducted by a DHS-funded partner under Section 3(a) of Executive Order 13691.²

As in the previous Executive Order 13636 assessments, the scope of this year's assessment is limited to those 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. 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, rather than attempting to assess the many DHS cybersecurity programs and activities conducted 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).³ 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 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 in order to be more transparent.

³ 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.⁴

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.⁵

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

⁴ 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>.

⁵ 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>.

Executive Order 13636 and Executive Order 13691 direct senior agency privacy and civil liberties officials of agencies engaged in activities under the orders to perform an “evaluation of activities against the Fair Information Practice Principles (FIPPs) and other applicable privacy and civil liberties policies, principles, and frameworks.”⁶ 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 1974,⁷ have served as DHS’s core privacy framework since the Department was established. They are memorialized in the DHS Privacy Office’s Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 2008)⁸ and in DHS Directive 047-01, Privacy Policy and Compliance (July 2011).⁹ The DHS implementation of the FIPPs is as follows:

Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a System of Records Notice (SORN)¹⁰ and Privacy Impact Assessment (PIA),¹¹ as appropriate. There should be no system the existence of which is a secret.

⁶ Section 5(a), E.O. 13636.

⁷ 5 U.S.C. § 552a

⁸ Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

⁹ 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.

¹⁰ The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding personally identifiable information (PII) collected in a system of records. A system of records means a group of records under the control of the agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. SORNs 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.

¹¹ The E-Government Act of 2002 (44 U.S.C. § 3501 note) 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

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 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 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

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.

DHS.¹² When conducting a Privacy Compliance Review (PCR)¹³, the Privacy Office evaluates the program's compliance with the FIPPs, any requirements outlined in its PTA, PIA, or SORN, and any privacy policies that are specific to that program. It is important to note, however, that because DHS uses the FIPPs as its foundational privacy policy framework, many DHS programs or activities do not require specific privacy policies aside from DHS's Privacy Policy Guidance Memorandum on the FIPPs, DHS Directive 047-01 "Privacy Policy and Compliance," and any specific privacy requirements documented in an applicable PTA, PIA, and/or SORN.

Civil Rights and Civil Liberties Assessment Framework

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

- Individual rights and constraints on government action provided for in the Constitution of the United States.
- Statutory protections of individual rights, such as the Civil Rights Act of 1964, 42 U.S.C. §§ 1981-2000h-6.
- Statutes that indirectly serve to protect individuals, such as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.
- Executive Orders, regulations, policies, and other rules or guidelines that direct government action and define the government's relationship to the individual in specific circumstances.
- Other sources of law, authority or policy 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 issues affecting individual rights raised by a program or activity. The most salient of the factual findings and

¹² 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.

¹³ 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.

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 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.¹⁴ In addition, the Department has sought the guidance of its Data Privacy and Integrity Advisory Committee (DPIAC)¹⁵ on cybersecurity-related matters. The DHS Privacy Office has briefed the DPIAC on cybersecurity-related matters in numerous public meetings. At the Chief Privacy Officer's request, the DPIAC issued a public report and recommendations on implementing privacy in cybersecurity pilot programs. The report, which was issued in November 2012, has informed the Department's development work in this area, and will serve as a guide for future assessments by the Privacy Office.

In this year's report, as noted, the DHS Privacy Office and CRCL report out on the activities that the Department has conducted under Sections 2(c) and 3(a) of Executive Order 13691 since its issuance in February 2015. After a thorough review, however, the DHS Privacy Office and CRCL concluded that there were no new DHS activities that were undertaken during the past Fiscal Year as a result of Executive Order 13636, nor were there any pre-existing Executive Order 13636 related DHS activities that were substantially altered during the past Fiscal Year to 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.

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

Background:

Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, builds upon the foundation established by Executive Order 13636 by encouraging the development of

¹⁴ 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>.

¹⁵ 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>

information sharing and analysis organizations (ISAOs)¹⁶ for sharing cybersecurity information and collaboration within the private sector and between the private sector and government. Specifically, Executive Order 13691:

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

The purpose of encouraging the development of ISAOs is to permit sharing of cyber threat information among a broader group of sharing and analysis organizations than is presently conducted. Current cyber threat information sharing among groups of this type is focused on Information Sharing and Analysis Centers (ISACs), which largely mirror the 16 Critical Infrastructure Sectors and the corresponding Sector-Coordinating Councils sponsored by DHS and the sector-specific agencies charged with protecting critical infrastructure. The DHS grant sponsoring the development of ISAO guidelines recognized that the need for sharing cyber threat information is not limited to Critical Infrastructure Sector entities and it often cuts across traditional sector identifications. Entities outside these Sectors or those that do not fit neatly within only one sector often did not participate in Sector-specific information sharing activities. Similarly, various public and private sector entities saw value in sharing and analyzing information based on geographic communities, such as regions, local communities, or locales where multiple sectors converge, such as airports and seaports. These factors led to the independent establishment of voluntary participation cyber threat information sharing and analysis organizations, or ISAOs, which have self-organized on a regional basis or around other common interests that do not fit within the existing individual Critical Infrastructure Sector

¹⁶ An ISAO is “any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of gathering and analyzing ... communicating or disclosing ... and voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents.” 6 U.S.C. § 131(5). ISAOs include ISACs. See, e.g., 6 U.S.C. § 148(d)(1)(B)(ii). More information on ISAOs can be found here: <https://www.isao.org>.

model. Expanding the scope of existing cybersecurity information sharing – with appropriate privacy and civil liberties safeguards – will enable the Department to provide robust support to diverse cybersecurity groups, including non-critical infrastructure industry or commerce interests, or other communities of interest working to voluntarily and collectively improve their cybersecurity posture.

The Department has begun efforts to implement Executive Order 13691 during Fiscal Year 2016. As a result, this year's report includes a privacy assessment of the Department's activities under 2(c) of the Order and an update on Section 3 activities. Although we are providing an update on Section 3 under the Order, our offices determined that there was no other DHS activity to assess as a part of this year's report. The ISAO Standards Organization is a DHS partner and was founded with the assistance of a DHS cooperative agreement. The cooperative agreement contemplates substantial programmatic involvement with the Standards Organization by DHS, but while DHS maintains oversight of the execution of the agreement, the ISAO standards organization works independently of the Department and is not led by, or under the control of DHS. Nevertheless our offices are providing a factual update regarding the formation of the ISAO Standards Organization and its efforts to develop the initial set of voluntary ISAO guidelines under Section 3 of this order. We are providing this information to ensure transparency and to set the stage for any future assessment of DHS activities that may involve the Department's work with the Standards Organization or the ISAOs.

III. EO 13691, Section 2(c): Sharing of Cyber-Related Information with ISAOs:

The National Cybersecurity and Communications Integration Center (NCCIC), established under section [227(b)] of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and [227] of the Act.

Background

As directed by Executive Order 13691, DHS is engaged in continuous, collaborative, and inclusive coordination with ISAOs via the DHS National Cybersecurity and Communications Integration Center (NCCIC), which coordinates cybersecurity information sharing and analysis amongst the Federal Government and private sector partners. Aside from ad hoc requests for assistance, DHS mainly accomplishes this cyber information sharing with ISAOs through two programs: the Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) Initiative.

Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing and complements ongoing DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. A key aspect of CISCP is bi-directional information sharing: CISCP partners submit indicators of

observed cyber threats and information about cyber incidents and identified vulnerabilities to DHS, which DHS then shares with other CISCP partners in an anonymized fashion. Upon receiving a submission, CISCP analysts¹⁷ redact any personal (if not directly related to a cybersecurity threat) or proprietary information (if necessary) and analyze the submission in collaboration with both government and industry partners to produce accurate, relevant, timely and actionable analytical products. Currently, those products take the form of:

- **Indicator Bulletins (IB):** Short, timely bulletins regarding new threats and vulnerabilities. These bulletins are sent several times a week in machine-readable formats. These formats enable faster parsing and analysis, resulting in faster action taken to thwart attacks and remediate vulnerabilities.
- **Analysis Report (AR):** More in-depth analytic product that ties together related threat and intruder activity, describing the activity, how to detect it, defensive measures and remediation advice.
- **Priority Alert (PA):** Focused on providing early warning of a single specific threat or vulnerability expected to have significant and far-reaching impact.
- **Recommended Practices (RP):** Product that provides a method for collaboratively defining and documenting a series of “best practice” recommendations or strategies

To join CISCP, participants (including ISAOs) are required to sign a Cooperative Research and Development Agreement (CRADA). Along with governing participation in CISCP, a signed CRADA may permit access to the NCCIC watch floor and allows for company personnel to be eligible for security clearances to view classified threat information.

In addition, ISAOs may connect to DHS’s AIS capability, which enables the exchange of cyber threat indicators and defensive measures between public and private entities at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated). Defensive measures are instructions or methods for defeating or defending against a cyber threat in a manner that does not cause damage to another machine. AIS is a part of the Department’s effort to create an ecosystem where as soon as an entity (such as a government agency or private sector company) observes an attempted compromise, the associated indicator will be shared in real time with all AIS participants, protecting them from that particular threat. This mechanism reduces the effectiveness or number of times adversaries can use the attack, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate the most sophisticated cyber threats, it will allow public and private entities to concentrate more on them by clearing away less sophisticated attacks. AIS is available for free to all private sector entities; federal departments and agencies; state, local, tribal, and territorial governments; information sharing and analysis centers (ISACs) and ISAOs; and foreign partners and companies.

To take part in AIS, AIS participants must sign the *AIS Terms-of-Use*¹⁸ and connect to a DHS-managed system in the Department’s NCCIC that allows bidirectional sharing of cyber threat

¹⁷ CISCP analysts are made up on analysts from DHS’s United States Computer Emergency Readiness Team (US-CERT).

¹⁸ See https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf

indicators. Each partner requires a technical capability (which can be built or bought from a number of commercial vendors) to allow them to exchange indicators with the NCCIC. Participants will not only receive DHS-developed indicators, but can also share indicators they have observed in their own network defense efforts, which DHS will then share back out to all AIS participants.

AIS leverages the Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII)¹⁹ specifications for machine-to-machine communication. Any entity participating in AIS must be able to communicate using these machine-to-machine specifications.

Privacy Assessment

FIPPs Analysis

Transparency: DHS exhibits a high level of transparency to the public regarding both the CISCIP and AIS programs. For example, information on CISCIP and AIS is available through DHS's public-facing website²⁰ and the published Privacy Impact Assessments (PIA) which cover the activities of these programs.

The PIA that covers CISCIP activities is **DHS/NPPD/PIA-026**, National Cybersecurity Protection System (NCPS), July 30, 2012.²¹ NCPS is an integrated system for intrusion detection, analysis, intrusion prevention, and information sharing capabilities used to defend the federal civilian government's information technology infrastructure from cyber threats. The National Protection and Programs Directorate (NPPD) conducted this PIA because PII may be collected by NCPS, or through submissions of known or suspected cyber threats received by the NCCIC for analysis.

AIS activities are covered by **DHS/NPPD/PIA-029(a)**, Automated Indicator Sharing (AIS), March 16, 2016.²² AIS enables the timely exchange of cyber threat indicators and defensive measures among federal and non-federal entities, to include ISAOs. NPPD conducted this PIA because PII may be submitted as part of or accompanying a cyber threat indicator or defensive measure.

Data Minimization: For contact information collected from individuals for CISCIP, DHS collects the minimum information necessary directly from the individuals. As a general rule, the NCPS only collects data that is necessary to accomplish its mission. For information collected from the person reporting an incident, analysts may attempt to confirm the integrity of the data received through the voluntary submissions by contacting the individual through phone or email. When provided, this includes the contact information of the person reporting the incident (if

¹⁹ See <https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity>.

²⁰ See <https://www.dhs.gov/ciscip> and <https://www.dhs.gov/ais>.

²¹ See <https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ncps-2015.pdf>

²² See https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_ais_update_03162016.pdf

applicable), incident data, which may include IP and host addresses and flow data, and actions taken to resolve the incident. Any information that is collected must be considered to be directly relevant and necessary to accomplish the specific purposes of the program; if it is not, the United States Computer Emergency Readiness Team (US-CERT) analyst is trained to notify the US-CERT Oversight and Compliance Officer and to delete it in accordance with US-CERT SOPs, which prohibit the sharing and storage of PII on the US-CERT.gov portal, and content is periodically reviewed by US-CERT analysts to ensure that no PII resides in the portal.

DHS also has strong safeguards in place for AIS to ensure that only PII that is related to a cyber threat is collected and retained. As a result, AIS has processes in place that:

- Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat;
- Incorporate elements of human review on select fields of certain indicators to ensure that automated processes are functioning appropriately;
- Minimize the amount of data included in a cyber threat indicator to information that is directly related to a cyber threat;
- Retain only information needed to address cyber threats; and
- Ensure any information collected is used only for network defense or limited law enforcement purposes.

Individual Participation: Participants in the CISCIP or AIS programs may contact the DHS/NCCIC directly if they wish to submit a correction to their PII collected for the purposes of signing up for CISCIP or AIS, signing the respective CISCIP CRADA or *AIS Terms-of-Use* agreements, or providing identity information as part of their indicator submissions.

However, an individual whose PII has been submitted as a part of the cyber threat may not correct his or her information. These individuals are not granted a right to access, correct, or amend these records under the Privacy Act because cyber threat indicators are not maintained in a System of Records. Individuals may still submit a Freedom of Information Act (FOIA) request to the DHS/NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. However, the Cybersecurity Information Sharing Act of 2015²³ (CISA) provides that cyber threat indicators and defensive measures shared with the Federal Government under CISA may be withheld from disclosure. Section 104(d)(4)(B) of CISA exempts cyber threat indicators and defensive measures from disclosure under any provision of state, tribal, or local freedom of information law and similar disclosure laws. Section 105(d)(3) of CISA exempts cyber threat indicators and defensive measures from disclosure under FOIA and withholds this information without discretion, from the public under Section 552(b)(3)(B) of FOIA.

Purpose Specification: As outlined in the CRADA signed by each CISCIP participant, CISCIP collects and shares cyber threat information to enable DHS and CISCIP participants (including ISAOs) data flow and analytical collaboration activities associated with cybersecurity, communications reliability, and cyber/communications crossover issues (e.g., control systems

²³ Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N § 104(c), 129 Stat. 2242, 2942 (2015), available at <https://www.congress.gov/114/bills/hr2029/BILLS-114hr2029enr.pdf>.

security, supply chain risk management, the transition of network to IP platforms, etc.) across the spectrum of security coordination including detection, prevention and mitigation of cyber threats to the security of critical infrastructure networks and systems.

In the *AIS Terms-of-Use*, DHS describes the purpose of AIS to be the exchange of timely, relevant, and actionable cyber threat indicators and defensive measures amongst and between AIS Participants and the Federal Government for a “Cybersecurity Purpose.” Section 102(4) of CISA defines a Cybersecurity Purpose to mean protecting an information system (of an AIS Participant, a customer or member of an AIS Participant, or otherwise) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. Cybersecurity Purpose includes research that is conducted for a Cybersecurity Purpose.

Use Limitation: For CISCP, DHS uses PII from CISCP participants to certify their agreement to the CRADA and to identify all points of contact who will be involved in the receipt and accountability of Federal Government analytic products provided.

As outlined in the CRADA, DHS and CISCP participants collaborate on cyber information sharing to:

1. enhance public-private data sharing and analytical collaboration related to cybersecurity, communications reliability, and related issues,
2. align existing detection capabilities related to security risks to protected cyber and communications systems,
3. prevent or mitigate risks to the Nation’s public and privately owned/operated protected systems,
4. participate in sector and cross-sector teleconferences, as needed, to facilitate cross-sector coordination activities,
5. improve the overall awareness, preparedness, and resilience of owners/operators of protected systems, and
6. build and maintain enhanced situational awareness.

In regards to AIS, DHS uses PII from AIS participants to certify their agreement to a Terms-of-Use, register or connect to TAXII, identify the submitter of web form or email submissions, and for consent (for the onward distribution of source-identity information). DHS uses information submitted via the AIS Profile²⁴ to disseminate computer-readable cyber threat indicators and defensive measures to federal and non-federal entities to supplement the existing mostly manual process.

AIS participants use disseminated cyber threat indicators and defensive measures for the uses authorized under CISA. Such authorized uses are limited to:²⁵

²⁴ See https://www.us-cert.gov/sites/default/files/ais_files/AIS_Submission_Guidance_Appendix_A.pdf

²⁵ Cybersecurity Act of 2015, Section 105(d)(5)(A).

1. a cybersecurity purpose;²⁶
2. the purpose of identifying (i) a cybersecurity threat, including the source of such cybersecurity threat, or (ii) a security vulnerability;
3. the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
4. the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or
5. the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in #3 above or any of the offenses listed in (i) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft), (ii) chapter 37 of such title (relating to espionage and censorship), and (iii) chapter 90 of such title (relating to protection of trade secrets).

Data Quality and Integrity:

As it relates to CISCP, where individuals voluntarily provide their name, email, phone number, and incident data, US-CERT may call or email the individuals to verify their information, security data, or to follow-up on a reported cyber incident submitted by the individual or organization. Individuals subscribing to US-CERT products have an interest in receiving the product information and individuals submitting an incident or malicious code information are often willing to provide further information in order to better support the information security community.

To assess the veracity of an incident that is reported to US-CERT, the analysts:

- 1) Capture incident data;
- 2) Verify the data through closed or open source research, e.g., Google, EINSTEIN flow data;
- 3) Contact the system owner;
- 4) Triage the incident, identify other affected parties, and contact them; and,
- 5) Work with the affected party or organization to identify a mitigation strategy.

However, with regard to sensor or other capability derived source, the hardware maintains exact copies of intrusion detection information transmitted to or from the federal network. For example, if a connection “spoofs” an IP address (manipulates the data packets it transmits to the federal network to appear as if being sent from one source when in fact they come from another source) the intrusion detection system will simply record those packets with the “spoofed” IP

²⁶ A Cybersecurity Purpose means protecting an information system (of an AIS Participant, a customer or member of an AIS Participant, or otherwise) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. Cybersecurity Purpose includes research that is conducted for a Cybersecurity Purpose.

address. The system only keeps a copy of the spoofed IP address; therefore, data collected by a sensor is accurate because it is an exact copy of the data available.

For AIS, the NCCIC is not able to validate the accuracy of every piece of information within an indicator or defensive measure submitted by an organization due to the sheer volume, anticipated workload, and timing necessary to ensure cyber threat indicators and defensive measures are shared in a real-time manner. AIS participants are required to adhere to submission guidance, which is provided to participating entities upon signing up for AIS, to ensure proper quality control of information submitted to AIS—in addition to adhering to privacy and other compliance requirements. Per the *AIS Terms-of-Use*, DHS reserves the right to terminate access to AIS for repeated failure to abide by submission guidance.

Finally, through its automated and manual processes, AIS executes a series of automated analyses and technical mitigations that ensure that the indicator information DHS expects to receive is what is actually received. For example, an actual IP address appears in the IP address field instead of a string of text.

Security: The CRADAs between DHS and CISCP participants outline a number of provisions related to the security of shared cyber threat information including the protection of: Protected Critical Infrastructure Information²⁷ (PCII), proprietary information,²⁸ and protected CRADA information.²⁹ In addition, these CRADAs outline requirements that CISCP participants with access to DHS networks or systems attend and comply with any required DHS training on data handling, protection, and management protocols, and provide notice to DHS of any inability to comply as soon as it is known. Lastly, information shared among CISCP partners is governed using the Traffic Light Protocol (TLP),³⁰ which empowers the submitter to determine the handling and dissemination of their information.

²⁷ Congress created the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information (CII) Act of 2002 to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security. Title II, Subtitle B of Pub. L. No. 107-296, available at https://www.dhs.gov/sites/default/files/publications/CII-Act_508.pdf.

²⁸ Proprietary Information” means Data that embodies trade secrets or commercial or financial Information and that: a) is not generally known, or is not available from other sources without obligations restricting its disclosure;

b) has not been made available by the owners to others without obligation restricting its disclosure;

c) is not described in an issued patent or a published copyrighted work or is not otherwise available to the public without obligation restricting its disclosure;

d) can be withheld from disclosure under 15 U.S.C. § 3710a(c)(7)(A) and the Freedom of Information Act, 5 U.S.C. § 552(b)(4);

e) is marked as Proprietary Information in accordance with Article 12.2.4 of the CRADA; and

f) has not been developed independently by persons who have had no access to the Information.

²⁹ “Protected CRADA Information” means Generated Information that is marked as being Protected CRADA information by a Party to the Agreement and that would have been Proprietary Information had it been obtained from a non-Federal entity.

³⁰ See <https://www.us-cert.gov/tlp>

As it relates to AIS, DHS ensures the appropriate distribution of AIS cyber threat indicators and defensive measures through the use of data tagging and access controls specification. These tools ensure that only the appropriate entities receive AIS indicators and defensive measures and source identity information is only shared with those entities when the AIS participant has provided consent. Non-federal entities accessing cyber threat indicators and defensive measures through AIS are subject to the *AIS Terms-of-Use*. These prescribe ground rules that non-federal entities must follow and submission guidance with which these entities must strive to adhere in regards to cyber information sharing.

Accountability and Auditing: Since CISCPC utilizes NCPS systems, DHS follows NCPS' accountability and auditing measures. Therefore, users must obtain a favorable DHS suitability determination³¹ prior to acquiring access to certain NCPS systems. All NCPS users supporting the program have a valid requirement to access the systems and only the type of access required to meet their professional responsibilities. Access is based upon the role identified on the access form (e.g., analyst, user, general user, system admin., network admin.). The NCPS access form must be completed by the government supervisor within the branch that the individual will be supporting. The user's role is defined by the branch manager and validated by the ISSM/Security Manager. Accounts are reviewed monthly by the ISSO to ensure that accounts are maintained and current. In addition, user account activity is logged, and the logs are reviewed each day. Users accessing EINSTEIN and the US-CERT portal through which NCPS disseminates information are adjudicated through their own organization.

US-CERT also maintains SOPs on privacy protection for the purpose of identifying sensitive information, and for the proper handling and minimization of PII, which outlines the necessary procedures and defines the terms, for specifically identified roles and responsibilities. These SOPs are provided to all US-CERT employees during training and are circulated to US-CERT analysts so that they are aware of what information should and should not be shared with its information sharing partners.

To ensure US-CERT employee adherence to these policies and procedures, DHS conducts bi-annual privacy oversight reviews. These reviews assess US-CERT employees' handling of PII for CISCPC and determine whether the handling of PII was consistent with those rules and procedures.

ISAOs participating in CISCPC are responsible for providing accountability and auditing measures for their own systems. The CRADA that ISAOs must sign, however, does require that they not provide PII in any of their submissions unless that information is necessary to identify or mitigate a cybersecurity, communications reliability, or related threat.

The AIS initiative follows the same procedures as identified for NCPS. In addition, the AIS Submission Guidance and *AIS Terms-of-Use* provide requirements to ensure information is being

³¹ The suitability determination is a process that evaluates federal or contractor employees' personal conduct throughout their careers. Suitability refers to fitness for employment or continued employment referring to identifiable character traits and past conduct that is sufficient to determine whether or not an individual is likely to carry out the duties of the position with efficiency, effectiveness, and in the best interests of the agency.

appropriately submitted to AIS. DHS also employs technical and manual mitigations and sanitization procedures, which provide additional assurance that PII not directly related to the cybersecurity threat is removed from the submission. In addition, DHS will periodically audit and review the submission history of AIS participants and their compliance with *AIS Terms-of-Use* and submission guidance. The audit and review will also be to ensure the technical mitigations are working appropriately and that the NCCIC analysts are appropriately sanitizing indicators and defensive measures.

IV. EO 13691, Section 3(a): ISAO Standards Organization Formation and Standards:

The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

As described in the Fiscal Year 2015 E.O. 13636 / E.O. 13691 Privacy and Civil Liberties Assessment report, the University of Texas at San Antonio (UTSA), with support from Logistics Management Institute (LMI) and the Retail Cyber Intelligence Sharing Center (R-CISC), was selected by DHS to serve as the ISAO Standards Organization (“Standards Organization”) under Section 3(a) of Executive Order 13691. Since the award process, the Standards Organization has been continuously working with existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs.³² As a part of its work towards identifying a common set of ISAO standards or guidelines (“standards”) in Fiscal Year 2016, the Standards Organization hosted several in-person, public meetings to solicit input from the public, industry sectors, government, and academia on the following dates and locations:

- November 9, 2015, Tysons, VA;
- February 9, 2016, UTSA;
- May 18-19, 2016, Anaheim, CA; and,
- August 31-September 1, 2016, Tysons, VA.

In addition to these in-person meetings, the Standards Organization also held online meetings on:

³² 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/>.

- December 18, 2015;
- January 21, 2016;
- March 10, 2016;
- April 19, 2016;
- July 21, 2016;
- September 22, 2016; and,
- September 29, 2016.

The earliest meetings in 2016 established the development process, set out a suggested “straw man,” provided the working draft standards to participants, and solicited assistance in the formation of working groups to develop standards in specific focus areas. The working groups were led by the Standards Organization, but were open to the public and typically composed of subject matter experts from various backgrounds. A mix of open and closed forum meetings led to the establishment of six Standards Working Groups (SWGs). The Standards Organization asked the SWGs to answer a series of questions in drafting the initial standards, including:

- What needs to be considered by a newly forming ISAO and what are the first steps?
- What capabilities might an ISAO provide?
- What types of information will be shared and what are some mechanisms for doing so?
- What security and privacy is needed for a newly forming ISAO?
- What mentoring support is available for newly forming ISAOs?
- What government programs and services are available to assist ISAOs?

The SWGs were also asked to consider public input, and what would be most useful for a group seeking to form an ISAO, when determining what information should be provided as part of the initial standards.

The Standards Organization published its first rough drafts of the proposed standards on May 3, 2016, and invited and received public comment for the next six weeks. The meeting of the Standards Organization held on May 18-19 focused on these drafts, and was open to the general public. It attracted over 100 attendees from multiple industry sectors, government, and academia.

After the first comment period closed, the Standards Organization and SWGs revisited the draft ISAO standards in light of public input, releasing edited versions for the August 31-September 1 in-person public meeting held in Tysons, VA. Following that meeting, and additional input from the public, the Standards Organization released the initial set of ISAO standards and guidelines on September 30, 2016 to include:

- ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs)
- ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)
- ISAO 300-1: Introduction to Information Sharing
- ISAO 600-2: US Government Relations, Programs, and Services

Each voluntary guidelines document sets forth high level goals and initial standards for the establishment and operation of ISAOs, with each hundred-series designation signifying a separate guidelines topic area. Subsequent guidelines will be issued to amplify and expand on the initial guidelines, and yet-to-be-published guidelines will also include voluntary standards in additional topic areas, such as analysis. The guidelines are anticipated to increase in number and evolve over time as ISAOs become more common, and as more feedback and public comments are received. DHS is not undertaking a detailed analysis of the Standards Organization’s published ISAO guidelines or ISAO implementation for inclusion in this this year’s report, because the Standards Organization’s work is not an activity of the Department within the meaning of the requirements of Section 5 of E.O. 13691.

Section 1 of Executive Order 13691 directs that any DHS-supported information sharing conducted by ISAOs “must be conducted in a manner that protects the privacy and civil liberties of individuals...”³³ The initial guidelines address those concerns at a high level. For example, ISAO 100-1: Introduction to Information Sharing and Analysis Organizations (ISAOs) sets forth the principles behind ISAOs, provides a basic overview of ISAOs, and outlines which working groups and documents will deal with privacy issues. This introductory document also states that a key question for any ISAO to answer, when sharing information, is: “How will privacy be maintained?”

Additional ISAO guidelines deal with this question in greater depth. The ISAO 300-1 document, “Introduction to Information Sharing” guideline is considerably more detailed, containing discussions about the major aspects of information sharing relevant to ISAOs. ISAO 300-1 also contains a fairly detailed discussion regarding the importance of privacy controls and protections as it states:

Ensuring privacy protections is critical to the process of information sharing and will increase partners’ trust in the overall structure of the ISAO itself. Attention to privacy can help the ISAO to manage or eliminate barriers and concerns around voluntary sharing of its members and partners. While ISAO participants may vary in having individual privacy officers, it is critical the ISAO itself be capable of managing these issues. These outcomes support sustainable and continuously improving ISAO business performance and viability.³⁴

³³ Section 1, Executive Order 13691.

³⁴ ISAO 300-1 Introduction to Information Sharing, September 30, 2016 at 33.

This guideline discusses initial privacy protection in some depth, but a fuller discussion of privacy and information security standards is planned to be issued as an ISAO 400-series guideline.

DHS leaders and staff periodically attended meetings hosted by the Standards Organization and were available to answer questions about DHS resources and activities; however, DHS's involvement in the actual development of the initial voluntary guidelines and standards for ISAOs was limited. The drafts of the initial standards were developed through an open, transparent, consensus-based process and represent the collaboration of over 160 experts from industry, government, and academia, combined with input and feedback from the public. Section 5(b) of Executive Order 13691 defines the scope of this portion of this assessment report. It requires "[s]enior privacy and civil liberties officials for agencies engaged in activities under this order [to] conduct assessments of their agency's activities." Because the ISAO standards were not produced by DHS but by an awardee, with limited DHS input, we do not consider the drafting process or the standards to be an activity of the Department.

As previously mentioned, DHS is not undertaking a detailed analysis of the Standards Organization's published ISAO guidelines or ISAO implementation for inclusion in this year's report because the Standards Organization's work is not an activity of the Department within the meaning of the requirements of Section 5 of E.O. 13691. Nevertheless, we are satisfied with the Standards Organization's treatment of privacy and individual rights protections thus far. The four published guidelines touch on the topic at a level of detail that is appropriate to the respective documents, provide initial rules of the road for ISAOs and further recommend voluntarily participating entities enact specific protections of privacy that are not inconsistent with the Department's approach to minimization and handling of personally identifiable information and the sharing of cyber threat information.

The DHS Privacy Office and CRCL will continue to monitor the progress of the Department's Executive Order 13691 activities and will assess these activities, as appropriate, in future Privacy and Civil Liberties Assessment Reports.

Part II: U.S. Department of Defense





OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

Ms. Veronica Venture
Acting Officer for Civil Rights and Civil Liberties
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Venture:

As the Department of Defense (DoD) Privacy and Civil Liberties Officer, I write this update on the activities of the Defense Industrial Base (DIB) Cybersecurity (CS) Program during Fiscal Year (FY) 2016, October 1, 2015 through September 30, 2016. This letter is submitted in accordance with the requirements of Executive Order (E.O.) 13636, “Improving Critical Infrastructure Cybersecurity”³⁵ and Presidential Policy Directive 21 (PPD-21), “Critical Infrastructure Security and Resilience.”³⁶

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

PPD-21 designates the DoD as the Sector-Specific Agency for the DIB, which is the DoD, U.S. Federal Government, and private-sector worldwide industrial complex with capabilities to design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts and perform research and development to meet military requirements. The DoD established the DIB CS Program to enhance and supplement DIB companies’ capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

This is DoD’s fourth submission to the E.O. 13636 Privacy and Civil Liberties Assessment Report and supplements the Department’s privacy and civil liberties assessments of

³⁵ Available at <https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

³⁶ Available at <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

the DIB CS Program contained in the 2014³⁷ and 2015³⁸ reports and DoD's letter to the 2016³⁹ report.

The DoD submission to the 2014 report assessed the activities of the DIB CS Program⁴⁰ based upon the Fair Information Practice Principles (FIPPs). For the 2015 report, the DoD refined its privacy and civil liberties assessment of the DIB CS Program by incorporating constructive feedback and suggestions provided by the Privacy and Civil Liberties Oversight Board. Both assessments concluded that the DIB CS Program protects our Nation's critical infrastructure from cyber threats in a manner that preserves individual privacy and civil liberties. For the 2016 report, the DoD submitted a letter in lieu of an assessment describing key DIB CS Program activities carried out in accordance with privacy and civil liberties safeguards during the reporting period.

The DIB CS Program policies and procedures did not substantially change during the reporting period for the 2017 report; however, a few notable improvements to the Program and its privacy and civil liberties safeguards are worth mentioning.

During the reporting period, industry participation in the DIB CS Program expanded from 128 to 185 companies. In the standardized agreement signed by the DoD and DIB companies, all parties agree to comply with Title 32 of the U.S. Code of Federal Regulations (CFR), part 236, "Department of Defense (DoD) Defense Industrial Base (DIB) Cyber Security (CS) Activities,"⁴¹ which "establishes "a comprehensive approach to require safeguarding of covered defense information on covered contractor information systems and to require contractor cyber incident reporting," and conduct their respective activities "in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data." 32 CFR part 236 also states that the "[c]onfidentiality of information that is exchanged under the DIB CS program will be protected to the maximum extent authorized by law, regulation, and policy."

The DIB CS Program updated the Privacy Impact Assessment (PIA), "Defense Industrial Base (DIB) Cybersecurity Activities."⁴² A PIA must be completed for DoD information technology and electronic collections that collect, maintain, use, or disseminate personally

³⁷ Available at <http://www.dhs.gov/publication/executive-order-13636-privacy-and-civil-liberties-assessment-report-2014>.

³⁸ Available at <http://www.dhs.gov/publication/2015-executive-order-13636-privacy-and-civil-liberties-assessment-report>.

³⁹ Available at <https://www.dhs.gov/publication/executive-order-13636-privacy-civil-liberties-assessment-report-2016>.

⁴⁰ The "DIB CS/IA Program" was renamed the "DIB CS Program" during an alteration to the Program's System of Records Notice in May 2015.

⁴¹ Available at <http://www.ecfr.gov/cgi-bin/text-idx?SID=ecee1a270d6ffd1361d5b5f031030fae&mc=true&node=pt32.2.236&rgn=div5>.

⁴² Available at http://dodcio.defense.gov/Portals/0/Documents/PIA_DIB%20CS%20program_Aug%202015_corrected.pdf?ver=2016-09-22-113831-737.

identifiable information (PII).⁴³ The PIA for the DIB CS Program analyzes how DIB CS Program information is handled in compliance with applicable laws and policies, identifies potential privacy and security risks, and explains how these risks are mitigated to ensure the information is adequately protected.

The Privacy Act System of Records Notice (SORN), “Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records”⁴⁴ was modified to ensure it accurately describes the current state of the system of records that maintains cyber threat information for the DIB CS Program. SORNs provide public notice and transparency about personal information collected, used, disseminated, and maintained in a system of records. The modifications to the DIB CS Activities Records SORN include changes to the system name, system location, categories of records, authority for the maintenance, purpose, routine uses, retrievability, safeguards, system manager and address, notification procedure, record access procedure, and record source categories. The Department clarified that DIB CS Program cyber incident reports contained in the system are retrieved by incident number or company name and now notes that DIB company point of contact (POC) information is retrieved primarily by company name, work division/group, and secondarily by individual POC name. The routine use section also was updated to identify all non-DoD agencies and entities that can receive disclosures of DIB CS Program information without the consent of the individual to whom the record pertains if the receiving agency or entity’s purpose for the information is compatible with the DoD’s purpose for the information collection.

The DIB CS Program continued to comply with Paperwork Reduction Act (PRA)⁴⁵ requirements for information collections from members of the public, such as DIB company POCs, by submitting updated information collection requests to the Office of Management and Budget (OMB) for cyber incident reporting and cloud computing,⁴⁶ DIB CS Program cyber incident reporting,⁴⁷ and the application process for joining the DIB CS Program.⁴⁸ These

⁴³ See Public Law 107-347, 44 U.S.C. Ch 36 (E-Government Act of 2002); See also DoD Instruction 5400.16, (Change 1), “DoD Privacy Impact Assessment (PIA) Guidance,” August 11, 2017. Available at <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540016p.pdf?ver=2017-08-11-124058-600>.

“DoD Privacy Impact Assessment (PIA) Guidance,” July 14, 2015. Available at <http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf>.

⁴⁴ Available at <http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570553/dcio-01.aspx>.

⁴⁵ See 5 C.F.R. part 1320 (requiring Federal agencies to obtain OMB approval for certain collections involving 10 or more persons in a 12-month period regardless of format).

⁴⁶ See OMB Control Number 0704-0478, “Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing.” Available at http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201603-0704-003#.

⁴⁷ See OMB Control Number 0704-0489, “DoD’s Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting.” Available at http://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201609-0704-003.

⁴⁸ See OMB Control Number 0704-0490, “Defense Industrial Base Voluntary Cyber Security/Information Assurance Points of Contact (POC) Information.” Available at <http://www.reginfo.gov/public/do/PRAOMBHistory?ombControlNumber=0704-0490>.

OMB-approved information collections aid compliance with PRA and Privacy Act provisions by limiting the DoD's collection of PII to the minimum necessary for the DoD to contact DIB companies.

Finally, the DoD continued to refine mandatory cyber incident reporting requirements for defense contractors. The DoD published a final rule in the *Federal Register*, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018),⁴⁹ which implements 10 U.S.C. sections 391 and 393 requirements for cyber incident reporting by cleared defense contractors and those companies providing operationally critical support. The final rule incorporates changes made in two interim rules⁵⁰ and requires contractors to safeguard Covered Defense Information⁵¹ that “resides in or transits through covered contractor information systems.” Defense contractors rapidly report compromises of their unclassified networks or information systems to a single web portal⁵² using the same process for mandatory and voluntary reporting, while also ensuring that privacy and civil liberties protections continue to be effective. The rule also requires DoD contractors to implement the security requirements in NIST Special Publication 800-171.⁵³

The DIB CS Program is a public-private cybersecurity partnership designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness. The DoD will continue to comply with Federal law and DoD policies and protect individual privacy and civil liberties when the DoD and participating DIB companies collect and share DIB cybersecurity threat information.

David Tillotson III
DoD Privacy and Civil Liberties Officer

cc:
Mr. Sam Kaplan
Chief Privacy Officer

⁴⁹ See 81 FR 72986. Available at <https://www.gpo.gov/fdsys/pkg/FR-2016-10-21/pdf/2016-25315.pdf>.

⁵⁰ DoD published two interim rules in the Federal Register on August 26, 2015 (80 FR 51739) and December 30, 2015 (80 FR 81472).

⁵¹ Covered Defense Information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/categorylist.html>) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is: (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the agreement.

⁵² Available at <https://dibnet.dod.mil/>.

⁵³ NIST Special Publication 800-171 Revision 1, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” December 20, 2016.

Part III: U.S. Department of Justice





U.S. Department of Justice

Office of the Deputy Attorney General

Telephone: (202) 514-0208

Washington, D.C. 20530

August 8, 2017

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

Ms. Veronica Venture
Officer for Civil Rights and Civil Liberties (Acting)
U.S. Department of Homeland Security
245 Murray Lane, SW, M/S 190
Washington, DC 20528

Dear Mr. Kaplan and Ms. Venture:

I currently serve as the United States Department of Justice (DOJ or “the Department”) Acting Chief Privacy and Civil Liberties Officer (CPCLO) and the designated senior agency privacy and civil liberties official. Pursuant to Section 5(b) of Executive Order (EO) 13636 (February 12, 2013), Improving Critical Infrastructure Cybersecurity, I am pleased to provide you with this letter updating the Department’s privacy and civil liberties assessment on the Department’s critical infrastructure cybersecurity information sharing activities.

By way of context, EO 13636 directed 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. Section 5 of EO 13636 directs 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 the DHS CPO and DHS OCRCL to make recommendations to the DHS Secretary of ways to minimize or mitigate such risks in a publicly available report. This process requires the senior agency privacy

and civil liberties officials for the other agencies engaged in cybersecurity information sharing activities under the EO to conduct their own privacy and civil liberties assessment reports, and send their reports to DHS for consideration and inclusion in a government-wide EO 13636 Privacy and Civil Liberties Assessment Report.

In April 2014, the Department submitted its first privacy and civil liberties assessment of its cybersecurity information sharing activities under Section 4(a) and Section 4(b) of EO 13636. Since the inaugural 2014 assessment report, the Department has annually reviewed and revised its privacy and civil liberties assessment reports, as necessary. These assessment reports included a description of the Department's privacy and civil liberties framework, as well as the Department's cybersecurity framework. The Department engages in cybersecurity information sharing under 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.

I have determined that DOJ's activities under EO 13636 have not substantially changed since the Department's 2016 privacy and civil liberties assessment report, which covered fiscal year 2015.⁵⁴ The Department primarily engages in cybersecurity information sharing in accordance with EO 13636 through activities undertaken by the FBI's Cyber Guardian system. The Department's past EO 13636 assessment reports have primarily consisted of descriptions of the FBI-specific Cyber Guardian framework, and the assessments of the protections for privacy and civil liberties have related primarily to that system. Since there were no substantial changes to Cyber Guardian during the fiscal year 2016 reporting period, I have determined that the CPCLO's privacy and civil liberties assessment from last year did not need any substantial changes. This letter, however, updates and clarifies the Department's role in implementing certain provisions of EO 13636 during fiscal year 2016, and provides current information through July 2017. The Department participated in an interagency working group to coordinate the review and revision of the 2017 government-wide report. This working group is led by representatives from DHS, in collaboration with the White House's National Security Council (NSC). 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)

As noted above, Section 4(a) of EO 13636 establishes as the policy of the United States Government the requirement to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Section 4(a) also requires the DHS Secretary, the Attorney General (AG), and the Director of National Intelligence (DNI) to issue instructions to ensure the timely production of information about unclassified cyber threats to the U.S. homeland that identify a specific targeted entity ("cyber threat reports"). Again as noted, the

⁵⁴ The Department's 2016 EO 13636 Privacy and Civil Liberties Assessment Report, reflecting the fiscal year 2015 reporting period, is located at:

https://www.dhs.gov/sites/default/files/publications/2016%20EO%2013636%20Assessment%20Report-FINAL_0.pdf.

Department's activities under Section 4(a) have not substantially changed from those analyzed in its prior privacy and civil liberties assessments.⁵⁵

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, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. Finally, Section 4(b) of EO 13636 requires the DHS Secretary and the AG, in coordination with the DNI, to establish a system to track the production, dissemination, and disposition of these reports, the so-called "4(b) solution." While the Department's activities under Section 4(b) have not substantially changed from those analyzed in our prior assessments, I would like to highlight a number of noteworthy updates that have occurred during the reporting period, as well as further clarify aspects of Cyber Guardian.

As noted in the Department's 2016 privacy and civil liberties assessment report, the NSC, through the Cyber Interagency Policy Committee, authorized the FBI's National Cyber Investigative Joint Task Force (NCIJTF) to implement Section 4(b) of EO 13636 using Cyber Guardian, a sharing and integration platform. Cyber Guardian offers Federal Cyber Centers⁵⁶ and Intelligence Community (IC) partners the ability to coordinate a whole-of-government response to targeted entities and victims of cyber incidents identified in government intelligence collections. Through Cyber Guardian, government agencies with cyber missions are made aware of and able to de-conflict cyber incidents, both with respect to their resolution and in furtherance of the government's victim notification responsibilities.

The FBI has conducted a Privacy Impact Assessment (PIA) on Cyber Guardian that assessed the privacy risks in accordance with Section 208 of the E-Government Act of 2002,⁵⁷ Office of Management and Budget directives, DOJ policy, and specific FBI guidance.⁵⁸ Each of these requirements incorporates the Fair Information Practice Principles (FIPPs) (*e.g.*, transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing) in assessing how privacy and other protections are incorporated into Cyber Guardian. In addition, a FIPPs assessment of Cyber Guardian was included in the Department's 2016 privacy and civil liberties assessment report. An update tracking our last privacy and civil liberties assessment follows below:

⁵⁵ 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.

⁵⁶ Under the Enhance Shared Situational Awareness initiative, the following Federal Cyber Centers are developing an information-sharing framework and shared situational awareness requirements for sharing cybersecurity information: Defense Cyber Crime Center; Intelligence Community Security Coordination Center; National Cybersecurity and Communications Integration Center; NCIJTF; National Security Agency/Central Security Service Cyber Threat Operations Center (NCTOC); and United States Cyber Command Joint Operations Center.

⁵⁷ *See* 44 U.S.C. § 3501 (note) (2012).

⁵⁸ The PIA was approved by the DOJ Acting CPCLC on April 17, 2017.

- Critical Infrastructure Entity Access to Cyber Guardian Reports:** As indicated in the Department’s 2016 privacy and civil liberties assessment report, the Department anticipates that in the future Cyber Guardian will become a platform for threat reports to be assimilated and made available for direct dissemination to the private sector. The Department intends to have the capability to disseminate both unclassified and classified reports to targeted critical infrastructure entities authorized to receive them. To further clarify our last assessment report, while Cyber Guardian facilitates interagency coordination for the purpose of threat notification, its current functionality does not allow for the direct dissemination of Cyber Guardian reports to targeted entities. This functionality is still conceptual and under review by the Department. Currently, operators use information in Cyber Guardian to separately draft and disseminate reports to targeted entities through existing public reporting structures, such as Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) Reports.⁵⁹ Dissemination of these reports to targeted entities, whether or not prepared from reports tracked through Cyber Guardian, is subject to strict privacy and civil liberties protections. As indicated in last year’s FIPPs assessment of Cyber Guardian, the information submitted on the Cyber Guardian incident form relates to cyber incidents only, and the FBI strictly adheres to federal and Department information sharing procedures and safeguards for the information that it maintains. The FBI is subject to federal information privacy laws, such as the Privacy Act of 1974, as amended,⁶⁰ which permits the sharing of Privacy Act-protected information only with individual consent or under specified statutory exceptions. Currently, FBI’s Cyber Guardian has only been used for cybersecurity purposes, specifically coordinating victim notifications, based on the submissions received during the reporting period. New capabilities, as they are developed, will be assessed for privacy and civil liberties protections.
- Revised Notice Banners for Cyber Guardian Users:** During this reporting period, an additional warning banner was added to Cyber Guardian to strengthen the notice provided to users of the system’s use restrictions. Specifically, the additional warning banner notifies authorized users that they may only use Cyber Guardian information for intelligence and lead purposes, and that such information may only be used in written products or briefings with the advance authorization of the originating agency.
- Automated Capabilities to Improve Information Integrity and Accuracy:** As indicated in the Department’s 2016 privacy and civil liberties assessment report, the type of information submitted into Cyber Guardian is generally technical information regarding the cyber incident. Any contextual information submitted in a narrative form describing the incident must be relevant to the submission of the cyber incident, in accordance with the FBI’s Memorandum of Understanding (MOU) executed by each Cyber Partner. To further increase the integrity and accuracy of information submitted into Cyber Guardian, the NCIJTF and the FBI are implementing additional capabilities to allow for the automated ingest of certain information that, during the prior reporting

⁵⁹ For more information on FBI’s PINs and FLASH Alerts, readers can contact their local FBI Field Office and speak with their Cyber Task Force designees.

⁶⁰ 5 U.S.C. § 552a (2012).

periods, NCIJTF and FBI manually entered. For instance, FBI and NCIJTF attempted to automatically ingest data from the National Security Agency/Central Security Service Cyber Threat Operations Center via Structured Threat Information Expression messaging. However, several problems arose, and this automated process has recently been taken off-line to improve the messaging system. Once the problems are corrected in the near future, the NCIJTF expects to reintegrate and use the improved system.

- **NCIJTF Updates to the Joint Requirements Team Support Capability Requirements:** On April 10, 2015, the Joint Requirements Team (JRT), with guidance from the NSC, finalized a document titled, “Executive Order (EO) 13636 Section 4(b) Support Capability Requirements for Notification to Critical Infrastructure Targeted Entities.” As indicated in the Department’s 2016 privacy and civil liberties assessment report, this document was used as the starting point for the development of the requirements for the Section 4(b) process and to build an agreed-upon business process and technical solution to implement the Section 4(b) solution. During the reporting period, NCIJTF produced a document that expanded the original JRT requirements. This document was provided to the FBI’s Information and Technology Branch to further develop and enhance the current Cyber Guardian platform so that it can fully support the 4(b) initiative, including the direct preparation for and distribution of threat notification reports to targeted entities, described above. Development of these system changes is ongoing and is anticipated to be completed in the second quarter of fiscal year 2018. New capabilities, as they are developed, will be assessed for privacy and civil liberties protections.
- **SIPRNet⁶¹ Intelink-S Connection Access:** The Department’s 2016 privacy and civil liberties assessment report indicated that the FBI was in the process of making Cyber Guardian available to authorized Cyber Centers, designated Sector-Specific Agencies (SSAs), and other authorized government agencies that directly support the DOJ’s cybersecurity mission through the SIPRNet Intelink-S connection from their home agencies. This capability now exists and is functional.
- **Phase I Training Completed:** The Department’s 2016 privacy and civil liberties assessment report indicated that the FBI initiated Phase I of its Cyber Guardian training to all designated Federal Cyber Centers, select SSAs, and other select government agencies with a cybersecurity mission. During this reporting period, Phase I training was finalized, however, training for United States Cyber Command and the Central Intelligence Agency (CIA) has not yet been completed.⁶² Employees who have not received Cyber Guardian training will not gain access to Cyber Guardian. NCIJTF is currently working to bring these agencies online, as well as other agencies that have participated in training or signed an MOU to govern their access but have not yet completed all of the requirements for access to Cyber Guardian, described below.

⁶¹ 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.

⁶² Some CIA employees, however, have access through their affiliation with the Cyber Threat Intelligence Integration Center (CTIIC). CTIIC has signed an MOU for Access to Cyber Guardian, and its affiliates have completed the necessary training and access requirements.

- **User Access Auditing Completed:** As indicated in the Department's 2016 privacy and civil liberties assessment report, access to Cyber Guardian requires users to satisfy a number of requirements, including: (1) complete on-site Cyber Guardian training; (2) review, sign, and return the FBI Rules of Behavior for Other Government Agency Personnel Authorized to Access Cyber Guardian (FD-889d); (3) possess and provide a valid Intelink Passport account (if accessing through SIPRNet); and (4) obtain Agency Head authorization and signature on FBI's MOU for Access to Cyber Guardian. During fiscal year 2016, a user audit was conducted that confirmed that all active system users have satisfied all requirements.

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. In this connection, the protection of privacy and civil liberties has been carefully integrated into all of DOJ's activities as it implements 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)

Part IV: Office of the Director of National Intelligence



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

December 2, 2016

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

Mr. Jonathan Cantor
Chief Privacy Officer (Acting)
Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Mack and Mr. Cantor:

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, 2016.

This is our fourth review under EO 13636. Our first assessment was submitted on December 2, 2013 for inclusion in the first Department of Homeland (DHS) Cyber Report, published in April 2014. In that initial submission, we included a comprehensive assessment of the ODNI's cyber activities under EO 13636. Beginning with our second review, submitted in February 2015, covering the period ending September 30, 2014 for inclusion in the second DHS Cyber Report, published in April 2015, we focused on relevant updates to previous years' reviews. We did the same for the third review submitted on January 22, 2016 covering the period ending September 30, 2015 for inclusion in the third DHS Cyber Report, published in April 2016. In this review, we again focus on relevant updates. For those interested in the original comprehensive assessment, please see the first DHS Cyber Report dated April 2014.

Our submission last year indicated that we would assess the activities of the newly-created Cyber Threat Intelligence Integration Center (CTIIC), established by presidential memorandum in February 2015 and authorized and funded by Congress in December 2015. I assigned a CTIIC Civil Liberties and Privacy Officer (CTIIC CLPO) to provide civil liberties and privacy guidance to CTIIC personnel. Because CTIIC focuses on providing integrated analytic products to other government agencies, the CTIIC CLPO trained all CTIIC personnel regarding rules for disseminating information that contains information identifying or concerning a U.S. person (USPI).

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.” Additionally, CTIIC does not foresee being directly involved with cyber tearline reporting as the tearlines are produced by the information originator. 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

Part V: U.S. 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 constitutes a review of Department of Energy's (DOE) privacy and civil liberties activities under Section 5 of the E.O. for the fiscal year ending September 30, 2016. 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 Delivery and Energy Reliability (OE), the lead office for the Smart Grid, in coordination with the Federal Smart Grid Task Force (Task Force), continues to work closely with Smart Grid stakeholders to protect the privacy of consumers' customer data. As reported last year, DOE has no jurisdiction to either regulate or monitor utilities or third-party entities that collect or use energy usage data.

In 2016, DOE's Voluntary Code of Conduct (VCC) Initiative (discussed in DOE's 2016 E.O. 13636 report) was rebranded as the [DataGuard|Energy Data Privacy Program](#) (DataGuard). Private sector companies that adopt the VCC receive guidance on the sharing, access, and protection of consumer energy use data.

Recent developments and upcoming DataGuard initiatives include:

- The U.S. Patent and Trademark Office (USPTO) approved DOE's application to establish a DataGuard certification trademark. The application summary was published on the USPTO website on February 7, 2017, subject to clearing a 30-day objection period. DataGuard staff are waiting to receive a final report from the USPTO following the conclusion of the comment period. If no objections are filed, the DataGuard certification mark will become officially registered. Once the certification mark is registered, participating companies and entities will be able to brand their websites and possibly products with the certification mark, which, DOE believes, will be useful for consumers interested in the protection of their personal data.
- DOE manages a DataGuard Revisions Working Team (RWT), comprised of volunteer stakeholders from a variety of organizations spanning the private, public, and non-profit sectors. The RWT is responsible for conducting an independent review of the DataGuard initiative and the VCC concepts and principles every two years. The next RWT review process is expected to take place in 2017. DOE OE will follow a process similar to the process used to develop the initial VCC and related concepts and principles guidance, which included publication of notices in the *Federal Register*, convening open meetings, and RWT participation in industry working group meetings.

DOE OE also manages DOE participation in the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a Federal government Energy Sector collaboration that results in timely bi-directional sharing of threat information between government and industry. CRISP also develops and deploys situational awareness tools to enhance the Energy Sector's ability to identify threats and coordinate the protection of critical infrastructure. In 2016, CRISP continued to expand under the management of the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center (E-ISAC). NERC is currently conducting its first independent audit of CRISP's data handling procedures through on-site inspections.

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/>
- *Data Privacy and the Smart Grid: A Voluntary Code of Conduct*
https://www.dataguardprivacyprogram.org/downloads/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf
- Energy Sector Cybersecurity Preparedness (CRISP)
<https://energy.gov/oe/energy-sector-cybersecurity-preparedness-0>

Part VI: U.S. Department of Health and Human Services





July 24, 2017

Officer Megan H. Mack
Department of Homeland Security
Office for Civil Rights and Civil Liberties
Mailstop 190
245 Murray Lane, SW Building 410
Washington, D.C. 20528

Jonathan R. Cantor
Chief Privacy Officer (Acting)
U.S. Department of Homeland Security
245 Murray Lane, SW, M/S 0655, WDC 20528
Washington, D.C. 20528

Dear Ms. Mack and Mr. Cantor,

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, 2016. The Department’s previous assessments were submitted for inclusion in the DHS Cyber Reports for fiscal year (FY) 2014 and FY 2015, 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. In our investigations, we found that the activities that might appear to be subject to the reporting requirement are limited to developing guidance for the healthcare sector, rather than an internal program facilitated or run by HHS.

The 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

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

Part VII: U.S. Department of the Treasury





DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

November 9, 2017

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

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, 2015 to September 30, 2016 reporting period.

Treasury's activities under the EO have not materially changed since we last reported. Last year's assessment included a comprehensive privacy and civil liberties assessment using the Fair Information Practice Principles. This year, because our activities have not substantively changed we decided not to include a privacy and civil liberties assessment. Instead, we are providing a brief summary of our activities under the EO.

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 (“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 by 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 shared cyber threat information with the financial services sector in the form of unclassified Cyber Information Group (CIG)⁶³ 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. PTR started, but has not yet completed the retention schedule for the cyber information shared in CIG Circulars, PTR expects completion of the schedule during the 2018 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 privacy and civil liberties assessment of those activities in future reports.

Sincerely,

A handwritten signature in black ink, appearing to read "RLW", is centered below the word "Sincerely,".

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

⁶³ 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.