Audit Report

OIG-16-038

CYBERSECURITY: Department of the Treasury's Activities to Protect Critical Infrastructure in the Financial Services Sector

April 28, 2016

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations

Voluntary Program	Critical Infrastructure Cyber Community Voluntary Program
CIPAC	Critical Infrastructure Partnership Advisory Council
Commerce	Department of Commerce
DHS	Department of Homeland Security
EO	Executive Order
FBIIC	Financial and Banking Information Infrastructure Committee
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
HSPD-7	Homeland Security Presidential Directive 7
ITF	Integrated Task Force
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OCIP	Office of Critical Infrastructure Protection and Compliance Policy
PPD-21	Presidential Policy Directive 21
R&D	research & development
SCC	sector coordinating council
SLTT	State, local, tribal, and territorial
SSA	sector-specific agency
Treasury	Department of the Treasury

This page intentionally left blank.

April 28, 2016

Amias Gerety
Acting Assistant Secretary for Financial Institutions

This report presents the results of our audit of the Department of the Treasury's (Treasury) activities under Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, and Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. PPD-21 establishes a national policy on critical infrastructure security and resilience and designates Treasury as the sector-specific agency (SSA) for the financial services sector. EO 13636 directs the establishment of a framework to reduce cyber risks to critical infrastructure.

Our audit objective was to determine whether Treasury fulfilled its role and responsibilities as SSA for the financial services sector and met the requirements of PPD-21 and EO 13636. To accomplish our objective, we interviewed officials with Treasury's Office of Critical Infrastructure Protection and Compliance Policy (OCIP) and officials with the Department of Homeland Security (DHS) responsible for coordinating SSAs involved in protecting the Nation's critical infrastructure. We also reviewed documents related to Treasury's role as SSA for the financial services sector and its coordination efforts with government and private-sector entities. We conducted our fieldwork from December 2013 through March 2016. Appendix 1 contains a more detailed description of our objective, scope, and methodology.

In brief, we concluded that as SSA to protect critical infrastructure in the financial services sector, Treasury met the obligations of PPD-21 and EO 13636, as of March 2016. Specifically, Treasury coordinated with DHS and provided information to DHS necessary to meet its reporting requirements under PPD-21 and EO 13636. In addition, DHS will be required to report to the President the extent of private sector participation in a voluntary program intended to show support for the adoption of a Cybersecurity Framework.

Treasury plans to assist DHS with this anticipated reporting requirement for the financial services sector.

We are not making any recommendations to Treasury as a result of our review. We provided a draft of this report to Treasury for its review. In a written response, which is included as Appendix 2, Treasury agreed with our findings and stated that it will continue to work to fulfill its responsibilities.

Background

The Nation's critical infrastructure provides essential services that support American society. Critical infrastructure includes systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The cyber threat to critical infrastructure continues to grow, presenting one of the most serious national security challenges to the United States. Cyber-attacks on our financial system represent a threat to our economic and national security. In response to such cyber-attack threats that could disrupt our Nation's critical systems, the President signed EO 13636 and issued PPD-21[1] on February 12, 2013.

The implementation of PPD-21 and EO 13636 is intended to drive action toward system and network security and resiliency, and also enhance the efficiency and effectiveness of the Federal government's work to secure the Nation's critical infrastructure and make it more resilient. PPD-21 established a national policy on critical infrastructure security and resilience, which is a shared responsibility among Federal entities; State, local, tribal, and territorial (SLTT) entities; and public and private owners and operators of critical infrastructure. The policy's goals were to enhance overall coordination and collaboration and clarify the functions, roles, and responsibilities related to critical infrastructure

[1] PPD-21 revoked Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization and Protection.

across the Federal government. PPD-21 identified SSAs to provide institutional knowledge and specialized expertise about their sector while executing this directive's goals.

EO 13636 was established to enhance the security and resilience of the Nation's critical infrastructure; and to maintain a cyber environment that promotes safety, security, business confidentiality, and privacy through a partnership with the owners and operators of critical infrastructure. These partnerships will improve cybersecurity information sharing and collaboratively develop and implement risk-based standards. As part of EO 13636, SSAs were required to be consulted in the development and adoption of the cybersecurity framework.

PPD-21 identifies Treasury as SSA for the financial services sector. Treasury fulfills this role through OCIP.[2] OCIP collaborates and coordinates with the public- and private-sectors through meetings, conference calls, e-mails, and workshops. This office provides information needed by DHS to meet reporting requirements specified within these policies.

Results of Audit

Treasury Fulfilled Its Role and Responsibilities and Met the Requirements of PPD-21 and EO 13636

We concluded that as SSA for the financial services sector, Treasury met the obligations of PPD 21 and EO 13636, as of March 2016. Specifically, as required by PPD-21, Treasury carried out the following roles and responsibilities:

- coordinated with DHS and other relevant Federal departments and agencies and collaborated with critical infrastructure owners and operators, independent regulatory agencies, and SLTT entities, as appropriate;

[2] OCIP was formed in late 2002 by the Assistant Secretary for Financial Institutions following the events of September 11, 2001.

- served as a day-to-day Federal interface for the dynamic prioritization and coordination of financial sector specific activities;

- carried out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;

- provided, supported, or facilitated technical assistance and consultations for the financial services sector to identify vulnerabilities and help mitigate incidents, as appropriate; and

- supported the DHS Secretary with statutorily required reporting by providing annual financial services sector critical infrastructure information.

Overall, as of March 2016, we determined that Treasury coordinated with, and provided information to DHS as required under PPD-21 and EO 13636. As discussed below, DHS will be required to report to the President the extent of private sector participation in a voluntary program intended to show support for the adoption of a Cybersecurity Framework established under EO 13636. To that end, Treasury plans to assist DHS with this anticipated reporting requirement for the financial services sector.

Treasury's Coordination and Collaboration Efforts

OCIP officials informed us that they are in frequent communication with DHS, through formal meetings and ad-hoc communications. Meetings are attended by Treasury officials and representatives who are communicating technical information with DHS and private-sector partners. For example, during the Heartbleed virus incident that occurred in April 2014,[3] Treasury engaged with DHS for up-to-date information about the virus and disseminated that information to its private-sector partners.

[3] Heartbleed is a virus in the encryption technology that many websites use to protect information such as names, addresses, passwords, and credit card numbers. The virus has been found in several websites for email, banking, online shopping, and social networking, and allows data to be obtained even if the site appears to be secure.

A DHS official informed us that DHS had routine interaction with Treasury through an Integrated Task Force (ITF),[4] comprising eight different working groups created to complete specific tasks.[5] Treasury was a participant in these working groups, along with DHS and the other SSAs, to address the requirements and deliverables under PPD-21 and EO 13636. According to the DHS official, key interactions with Treasury laid the groundwork for joint coordination meetings. Treasury also participated in weekly conference calls and security clearance requests made by DHS. Another DHS official stated that Treasury has been an active participant at multiple levels.

As part of its SSA responsibilities, Treasury maintained a partnership and collaborated with the Financial and Banking Information Infrastructure Committee (FBIIC).[6] FBIIC coordinates the efforts of Federal and State financial regulators to address critical infrastructure issues, including preparation for and response to cyber or physical attacks against the financial system or indirect attacks or events that may affect the sector. Treasury's Assistant Secretary for Financial Institutions chairs the FBIIC, and Treasury participated in meetings to assist private-industry and government partners and any other critical infrastructure practitioners in enhancing their preparation and resilience efforts. FBIIC members have regulatory authority over different sections of the financial services sector and address infrastructure protection issues through routine regulatory interactions.

To further promote information sharing throughout the financial services sector, Treasury maintained private-sector partnerships, primarily with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

[4] DHS established an ITF to coordinate interagency and public- and private-sector efforts and to ensure integrated and synchronized implementation across the homeland security enterprise.

[5] The working groups included: Stakeholder Engagement, Cyber-Dependent Infrastructure Identification, Planning and Evaluation, Situational Awareness and Information Exchange, Incentives, Framework Collaboration, Assessments: Privacy and Civil Rights and Civil Liberties, and Research and Development. These working groups were dissolved once the specific tasks were completed.

[6] Treasury's partnership with FBIIC was established by EO 13231, Critical Infrastructure Protection in the Information Age, Oct. 16, 2001. FBIIC consists of 18 member organizations from across the financial regulatory community, both Federal and State. Under the EO, the committee is chaired by a designee of the Secretary of the Treasury.

(FSSCC)[7] and the Financial Services Information Sharing and Analysis Center (FS-ISAC).[8] FSSCC's members control the majority of assets in the financial services sector. Its mission is to strengthen resiliency against attacks and other threats to the sector's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the Federal government, and coordinating crisis response. The mission of FS-ISAC, in collaboration with Treasury and FSSCC, is to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents and to serve as the primary communications channel for the sector.

Reporting Requirements

PPD-21 and EO 13636 established several reporting requirements—most tasking DHS with the responsibility of issuing and reporting on the status of national critical infrastructure efforts. As SSA of the financial services sector, Treasury is required to support the DHS Secretary in meeting statutorily required reporting requirements by coordinating, collaborating, and providing sector-specific critical infrastructure information. The following summarizes Treasury's status in meeting those reporting and information requirements:

[7] FSSCC was created in June 2002 by the private sector, with recognition from Treasury and DHS, to coordinate critical infrastructure and homeland security activities in the financial services industry. It derives members from individual institutions, trade associations, and regional coalitions. More specifically, members represent the financial services sector, including: clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communications networks, financial advisory services, insurance companies, financial utilities, government and industry regulators, government-subsidized entities, investment banks, merchants, retail banks, and electronic payment firms.

[8] FS-ISAC was established in 1999 by the financial services sector to eliminate any significant vulnerability to both physical and cyber systems attached to the Nation's critical infrastructure. The FS-ISAC is owned by its members, which include banking firms, credit unions, securities firms, insurance companies, credit card companies, mortgage banking companies, financial services sector utilities, financial services service bureaus, appropriate industry associations, hedge fund IT, and security service providers. The FS-ISAC Board of Directors determines member eligibility, enforces member eligibility verification through trusted third parties, and oversees the operation of the FS-ISAC. The Board of Directors is elected by the membership to serve 3-year terms.

Reporting Requirements in PPD-21 (February 12, 2013):

- Critical Infrastructure Security and Resilience Functional Relationships: Within 120 days of the date of PPD-21 (June 12, 2013), through coordination with SSAs and other relevant Federal departments and agencies, the DHS Secretary was required to develop a description of the functional relationships within DHS and across the Federal government related to critical infrastructure security and resilience. This report was to serve as a roadmap for critical infrastructure owners and operators and SLTT entities to navigate the Federal government's functions for critical infrastructure security and resilience against both physical and cyber threats.

  In June 2013, DHS released a report entitled *Critical Infrastructure Security and Resilience Functional Relationships*, which described the existing functional relationships within DHS and across the Federal government related to critical infrastructure security and resilience. Treasury assisted in the preparation of this document by communicating and collaborating with DHS through meetings, phone calls, and emails. It also collaborated as a member of DHS's Situational Awareness and Information Exchange working group, which identified and mapped existing critical infrastructure security and resilience functional relationships across the Federal government.

- Evaluation of the Existing Public-Private Partnership Model: Within 150 days of the date of PPD-21 (July 12, 2013), the DHS Secretary, in coordination with SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, was required to analyze the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space.

  In July 2013, DHS issued a report entitled *Evaluation of the Existing Public-Private Partnership Model*, which included an analysis of how the existing public-private partnership model is working toward promoting the security and resilience of the

Nation's critical infrastructure. The analysis included recommendations to strengthen those partnerships.

Treasury was a participant of the Planning and Evaluation working group responsible for performing the analysis. Additionally, Treasury independently solicited and received input from critical infrastructure organizations in the financial services sector and other critical infrastructure groups, directly engaged with stakeholders, coordinated with other Federal agencies, and reviewed public comments from stakeholders at panels hosted by DHS and other private-sector groups.

- Identification of Baseline Data and Systems Requirements for the Federal Government to Enable Efficient Information Exchange: Within 180 days of the date of PPD-21 (August 11, 2013), the DHS Secretary, in coordination with SSAs and other Federal departments and agencies, was required to convene a team of experts to perform an analysis to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure.

  In August 2013, DHS issued a report entitled *Baseline Data and System Requirements for the Federal Government to Enable Efficient Information Exchange*, which includes baseline data and system requirements intended to further the goals of PPD-21 and enable secure information sharing among Federal, SLTT, and private-sector entities. The report provided recommendations to facilitate the exchange of information on strengthening the security and resilience of critical infrastructure. Treasury was a participant of the Situational Awareness and Information Exchange working group tasked with addressing the baseline data and systems requirements. Treasury also assisted in the preparation of this report by communicating and collaborating with DHS through meetings, phone calls, and emails.

- Update to the National Infrastructure Protection Plan (NIPP): Within 240 days of the date of PPD-21 (October 10, 2013), the DHS Secretary, in coordination with SSAs, other relevant

Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, was required to provide to the President a successor to the NIPP. The plan was to include the identification of a risk-management framework for strengthening the security and resilience of critical infrastructure, the methods to be used to prioritize critical infrastructure, the protocols to be used to synchronize communication and actions within the Federal government, and a metrics and analysis process for measuring the Nation's ability to manage and reduce risks to critical infrastructure.

On November 8, 2013, DHS released *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*. Treasury was a participant of the Planning and Evaluation working group that worked to revise the NIPP. According to DHS officials, Treasury reached out to its private-sector partners and wrote portions of the NIPP. DHS officials said that many of Treasury's perspectives were incorporated in the writing process, noting that those areas provided the private-sector with continuity and a better understanding of the plan.

- National Critical Infrastructure Security and Resilience Research & Development (R&D) Plan: Within 2 years of the date of PPD-21 (February 12, 2015), the DHS Secretary, in coordination with the Office of Science and Technology Policy, SSAs, Department of Commerce (Commerce), and other Federal departments and agencies, was required to provide to the President a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan is to be issued every 4 years after its initial delivery, with interim updates as needed.

  In December 2014, DHS released the *National Critical Infrastructure Security and Resilience R&D Plan*. Treasury participated in the development of this plan by communicating with DHS and its public- and private-sectors on a frequent basis. Treasury officials also attended workshops held specifically for the R&D plan to give feedback and insight to be incorporated into the plan.

Reporting Requirements in EO 13636 (February 12, 2013):

Baseline Framework to Reduce Cyber Risk to Critical Infrastructure: Through the consultative process[9] established by the DHS Secretary, which includes SSAs, among others, the Director of the National Institute of Standards and Technology (NIST) was required to lead the development of a framework to reduce cyber risks to critical infrastructure (Cybersecurity Framework). The Cybersecurity Framework was to include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. Furthermore, the DHS Secretary, Director of National Intelligence, and the heads of other relevant agencies were to provide threat and vulnerability information and technical expertise in the development of the framework. The preliminary version of the Cybersecurity Framework was required to be published 240 days after the issuance of EO 13636 (October 10, 2013). The final version of the Cybersecurity Framework was required to be published by February 12, 2014, 1 year after the issuance of EO 13636.

The preliminary version of the Cybersecurity Framework was published for comment in August 2013, and the final version was issued on February 12, 2014. Treasury participated in the Framework Collaboration working group responsible for collaborating with NIST to develop, evaluate, and disseminate the Cybersecurity Framework. Treasury worked and consulted with DHS in the open review and comment process to help develop the framework, attending NIST workshops for stakeholders, and coordinating meetings with public- and private-sector partners about the workshops. Treasury worked

[9] EO 13636, Section 6, Consultative Process, required the DHS Secretary to establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. This process was to include the DHS Secretary engaging and considering the advice of the Critical Infrastructure Partnership Advisory Council (CIPAC), Sector Coordinating Councils (SCCs), critical infrastructure owners and operators, SSAs, other relevant agencies, independent regulatory agencies, SLTT entities, universities, and outside experts. CIPAC was established by DHS to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal government, the private-sector, and SLTT entities. SCCs are private-sector coordinating councils of owners and operators within a particular sector of critical infrastructure established by the NIPP or any successor document.

with NIST to address areas of concern and provided DHS with required threat and vulnerability information.

- Critical Infrastructure Cybersecurity Voluntary Program: The DHS Secretary, in coordination with SSAs, was required to establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities. SSAs, in consultation with the DHS Secretary and other interested agencies, were to coordinate with SCC to review the Cybersecurity Framework, and if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

  In February 2014, DHS launched the Critical Infrastructure Cyber Community Voluntary Program (Voluntary Program) to improve the resiliency of critical infrastructure cybersecurity systems by supporting and promoting the use of the Cybersecurity Framework. In SCC meetings, Treasury participated in efforts to assist the owners and operators of critical infrastructure to adopt the Cybersecurity Framework. Additionally, Treasury informed the private entities in the financial services sector about workshops offered by DHS on the implementation of the Cybersecurity Framework. After consulting with the sector and in cooperation with SCC, Treasury decided not to create financial services sector-specific framework implementation guidance. Treasury concluded that implementation guidance was not necessary due to the regulatory structure of the sector.

- Analysis of Incentives to Promote Participation in the Voluntary Program: Within 120 days of the date of EO 13636 (June 12, 2013), the DHS Secretary and the Secretaries of Treasury and Commerce were to make recommendations separately to the President. These recommendations were to be based on analysis of the benefits and relative effectiveness of incentives that would promote private-sector participation in the Voluntary Program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities. Additionally, the Secretaries of Treasury and Commerce were to make recommendations about

whether the incentives require new legislation or can be provided to participants under existing laws and authorities.

In June 2013, Treasury issued a report entitled *Cybersecurity Incentives Pursuant to Executive Order 13636*, which included recommendations based on an analysis of the effectiveness of the incentives to promote participation in the program. The recommendations included: (1) leveraging the framework to encourage critical infrastructure organizations to strengthen their cybersecurity practices and increase the flow of real-time information between the government and private-sector; (2) further studying whether adoption of the framework through the Voluntary Program could serve as a standard of conduct for systems' integrity and precautions; (3) leveraging the framework to promote existing Federal grant programs that fund basic research pertaining to cybersecurity; (4) offering technical assistance to encourage critical infrastructure organizations to adopt the framework; and (5) exploring ways to further accelerate approval of security clearances. The report also discussed which incentives would require new legislation.

- Identification of Critical Infrastructure at Greatest Risk: Within 150 days of the date of EO 13636 (July 12, 2013), the DHS Secretary was required to use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the DHS Secretary was to use the consultative process, discussed above, and draw upon the expertise of SSAs. SSAs were to provide to the DHS Secretary any information that DHS required to carry out its responsibilities. The DHS Secretary, through coordination with SSAs, was to then confidentially notify owners and operators of the critical infrastructure identified. The DHS Secretary was required to review and update the list of identified critical infrastructure under this section on an annual basis, and provide such a list to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

Treasury assisted in meeting this requirement by providing DHS with information on areas of the financial services sector that would be affected by a cybersecurity incident resulting in catastrophic regional or national effects on public health or safety, economic security, or national security. As requested by DHS, Treasury prepared sector-specific plans, which provided the financial services sector's strategy for working with public- and private-sector partners to identify, prioritize, and coordinate the protection of critical infrastructure. Treasury also participated in the consultative process through discussions and meetings and by reviewing and commenting on the notification letters sent by DHS to owners and operators of the critical infrastructure. In addition, Treasury participated in the annual update process by consulting with DHS on its designation of financial services sector companies. The 2014 process did not produce any changes. As of February 2016, the 2015 annual review and update was completed, resulting in four companies being added to the financial services sector list. DHS notified those companies by letter in February 2016.

Ongoing and Future Actions

- Annual Reporting to the President: SSAs are required to report annually to the President, through the DHS Secretary, on the extent of the Voluntary Program participation by owners and operators identified as critical infrastructure where a cybersecurity incident could reasonably result in catastrophic effects. As of March 2016, OCIP officials stated that they have not received any requests for, or guidance from, DHS or Office of Management and Budget regarding the reporting.
- Staffing and Human Resources: Treasury established the administrative functions needed to support, among other things, Treasury as SSA of the financial services sector. Treasury designed an organizational structure—OCIP—that accounts for its administrative needs. Treasury's Departmental Offices and the Office of Personnel Management were providing OCIP with human resource capabilities to support its staffing efforts aligned with that structure. The most recent organizational chart provided by OCIP officials showed that the office has 11 of its

current 16 positions filled. As of February 2016, OCIP had open positions for Deputy Director for Cyber Intelligence, an Administrative Management Specialist, a Senior Cyber Intel Analyst and two Information Technology Specialists.

* * * * *

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss the report, you may contact me at (202) 927-5776 or Dana Duvall, Audit Manager, at (202) 927-9648. Major contributors to this report are listed in Appendix 3.

/s/
Susan Barron
Director of Banking Audits

The objective of this audit was to determine whether the Department of the Treasury (Treasury) fulfilled its role and responsibilities as the sector-specific agency (SSA) for the financial services sector and met the requirements of Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, and Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. We performed our audit fieldwork in Washington, DC from December 2013 through March 2016.

To accomplish our objective, we reviewed:

- PPD-21 and EO 13636, including any related regulations and guidance;
- human resources information provided by the Office of Critical Infrastructure Protection and Compliance Policy (OCIP);
- various correspondence and communications between OCIP, the Department of Homeland Security (DHS), and public- and private-sector entities;
- Treasury information provided to DHS and to the public- and private-sectors;
- documentation related to DHS's Integrated Task Force working groups;
- DHS's guidance provided to SSAs;
- DHS's June 2013 report entitled *Critical Infrastructure Security and Resilience Functional Relationships;*
- DHS's July 2013 report entitled *Evaluation of the Existing Public-Private Partnership Model;*
- DHS's August 2013 report entitled *Baseline Data and System Requirements for the Federal Government to Enable Efficient Information Exchange;*

- National Institute of Standards and Technology preliminary 2013 and final 2014 *Framework for Improving Critical Infrastructure Cybersecurity;*

- documentation related to the Critical Infrastructure Cyber Community Voluntary Program;

- Treasury's June 2013 report to the President, *Cybersecurity Incentives Pursuant to Executive Order 13636;*

- DHS's 2013 *Incentives Study Analytic Report;*

- DHS's *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience; and*

- DHS's November 2014 *Critical Infrastructure Security and Resilience National Research and Development Plan.*

In addition, we interviewed:

- OCIP officials responsible for Treasury's coordination efforts; and

- DHS officials and personnel responsible for the coordination of the Nation's critical infrastructure protection among SSAs. Interviewed were the Deputy Director/Enterprise Performance Management, the Deputy Director/Strategy and Policy, and a Special Agent-Detailee from the United States Secret Service to the Sector Outreach and Programs Division.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

April 22, 2016

Susan Barron
Director of Banking Audits
Office of the Inspector General
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Ms. Barron:

Thank you for the opportunity to review the draft report entitled *Treasury's Activities to Protect Critical Infrastructure in the Financial Services Sector* (the Report). This letter provides the official response of the Department of the Treasury (Treasury).

The Report examines Treasury's activities under Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, and Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. We are pleased that the Report found that Treasury has fulfilled its responsibilities as the sector-specific agency for the financial services sector and met the requirements of PPD-21 and EO 13636. Treasury will continue to work to fulfill its responsibilities.

Thank you once again for the opportunity to review the Report. We look forward to continuing to work with your office in the future.

Sincerely,

Amias M. Gerety
Acting Assistant Secretary
for Financial Institutions

Dana Duvall, Audit Manager
Daniel Gerges, Auditor in Charge
Kevin Guishard, Program Analyst
Adelia Gonzales, Referencer

Department of the Treasury

Deputy Secretary
Acting Assistant Secretary for Financial Institutions
Office of Strategic Planning and Performance Management
Office of the Deputy Chief Financial Officer, Risk and Control Group

Office of Critical Infrastructure Protection and Compliance Policy

Director

Office of General Counsel

Attorney Advisor

Office of Management and Budget

OIG Budget Examiner

Treasury OIG Website

Access Treasury OIG reports and other information online:
http://www.treasury.gov/about/organizational-structure/ig/Pages/default.aspx

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx