National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 10, 2016
Ms. Carolyn Lerner
Special Counsel
Office of Special Counsel
1730 M Street, Suite 300
Washington, D.C. 20036-4505

Re: OSC File No. DI-15-1969

Dear Ms. Lerner:

The enclosed report is in response to your referral of allegations that the U.S. Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP), Infrastructure Information Collection Division (IICD) failed to: 1) conduct a damage assessment of the IP Gateway system for classification purposes, 2) ensure IP Gateway compliance with applicable information security standards, and 3) ensure information security when expanding access to state, local, tribal, and territorial users. The Office of Special Counsel received these allegations from a whistleblower, [redacted], former deputy director of IICD. I am the designated official responsible for providing your office DHS' report pursuant to 5 U.S.C. § 1213.

On February 12, 2016, OSC referred the above allegations and a request for an investigation to DHS Secretary Jeh Johnson. The DHS Office of Inspector General received these allegations and referred them to the NPPD Office of Compliance and Security (OCS) on March 21, 2016.

The NPPD OCS's investigation discusses at length the purpose of the IP Gateway and the various systems and protocol to protect this information. Although IICD did not create a written "damage assessment" of the IP Gateway, it took several other important steps to review the security of IP Gateway information, to follow applicable guidelines for review for classification the information included in the IP Gateway, and to follow other protocol for securing the information contained in the IP Gateway. In addition to these steps, upon receipt of [redacted] concerns in 2015, IP sought guidance and assistance from the DHS Chief Security Officer and the contracting entity which manages IP Gateway, Argonne National Laboratory (ANL). In May 2015, Assistant Secretary for DHS IP and Original Classification Authority, Caitlin Durkovich, issued a memo documenting the decision that the IP Gateway does not require classification. The memo notes that the decision was a result of consultation with the Chief Security Officer, similar system owners and DHS stakeholders, and an extensive review of the products contained on the IP Gateway. The Assistant Secretary also instructed the Chief Security Officer to establish guidelines for periodic review of IP Gateway to ensure regular assessment of the classification decision. Accordingly, the Agency does not plan additional corrective measures with respect to the first allegation. With respect to the second allegation, the

investigation revealed that IP Gateway meets information security standards established for high impact information systems as established by the National Institute of Standards and Technology (NIST) and the DHS 4300A Sensitive Systems Handbook. With respect to the third allegation, the investigation demonstrates that IP IICD officials took steps to ensure the security of information accessed through IP Gateway when it expanded access to SLTT government users. Accordingly, the Agency does not plan additional corrective measures with respect to the second and third allegations.

If you require further information regarding this matter, please contact Stephanie Sawyer in the Office of General Counsel at 202-447-3951.

Sincerely,

Suzanne E. Spaulding
Under Secretary
U.S. Department of Homeland Security
National Protection and Programs Directorate

Executive Summary

On March 21, 2016, the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Compliance and Security (OCS), Internal Affairs Division (IAD) received a referral from the DHS Office of Inspector General (OIG), which was referred from the Office of Special Counsel (OSC). The complaint originated from a former employee of NPPD's Office of Infrastructure Protection.

The complaint alleged that NPPD failed to adequately secure critical infrastructure information. The OSC identified three specific allegations for investigation related to the Infrastructure Protection Gateway (IP Gateway):

1. The Infrastructure Information Collection Division (IICD) failed to conduct a damage assessment of the IP Gateway to determine whether the collection of information available through the IP Gateway should be classified, and it failed to adequately assess individual items for classification.

2. IICD failed to ensure that the information security for the IP Gateway complies with applicable information security standards for high impact systems.

3. IICD failed to ensure the security of information accessed through the IP Gateway when it expanded access to state and local government users without ensuring compliance with information security standards.

Background Information

NPPD is a component of DHS. NPPD collaborates with federal, state, local, tribal, territorial (SLTT), international, and private-sector entities to maintain near real-time situational awareness of both physical and cyber events, share information about risks that may disrupt critical infrastructure, and build capabilities to reduce those risks. The Office of Infrastructure Protection (IP) is a sub-component within NPPD that leads and coordinates national programs and policies on critical infrastructure issues. IP has established strong partnerships across government and the private sector. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and state, local, tribal, and territorial partners understand and address risks. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage the risks to their assets, systems, and networks.

Within IP, the Infrastructure Information Collection Division (IICD) helps homeland security partners obtain and use needed infrastructure data. IICD accomplishes their mission, in part, via the IP Gateway. According to public information on the IP Gateway, information systems play a vital role in allowing federal, state, local, tribal, territorial, and private sector partners to identify, analyze, and manage risk to protect the nation. The IP Gateway serves as the single interface through which DHS partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis. This, in

turn, enables homeland security partners to quickly identify relevant vulnerability and consequence data in support of event planning, incident preparedness, and response efforts.[1]

Details of Investigation

Based upon the information provided by the OSC and the information provided by the complainant, the aforementioned allegations were investigated. To conduct the investigation, OCS interviewed the complainant, NPPD and DHS employees; reviewed e-mail records and other documents obtained during the investigation; reviewed relevant DHS and National Institute of Standards and Technology (NIST) policies and guidance documents pertaining to information security; and reviewed relevant DHS classification guides, Executive Orders, and various DHS OIG reports.

In addition to the complainant, OSC interviewed employees holding the following positions:

- NPPD, Director, IP Infrastructure Information Collection Division;
- NPPD, Director, IP Sector Outreach Programs Division;
- NPPD Chief Information Officer;
- NPPD Chief Information Security Officer/Director, Information Technology Security Division;
- DHS Office of the Chief Information Officer, Director of Policy, Architecture, and Governance;
- NPPD, Director, Office of Cyber and Infrastructure Analysis;

Summary of Findings

The NPPD Undersecretary and the Assistant Secretary of the Office of Infrastructure Protection possess delegated authority to make original classification decisions. The decision by an original classification authority is a discretionary decision. Information falling within Section 1.4 of Executive Order 13526 should not be subject to automatic classification. Over-classification causes confusion and negatively affects dissemination of information to SLTT and private sector partners. Over-classification is antithetical to the creation and operation of the information sharing environment established under the Intelligence Reform and Terrorism Prevention Act of 2004. Over-classification interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.

Although IP officials did not produce a document formally labeled as a "damage assessment," IP officials did, on various occasions and in various ways, assess the damage that could be caused by disclosure of information in the IP Gateway and took steps to ensure the security of the information. For example:

[1] https://www.dhs.gov/ipgateway.

- IP officials produce, periodically evaluate, and maintain security classification guides that determine when and what types of critical infrastructure information require classification for national security reasons. NPPD security classification guides are issued for the purpose of identifying specific topics of information associated with the protection of U.S. critical infrastructure that meets the standards and criteria for classification and protection in accordance with Executive Order 13526, "*Classified National Security Information*," and its implementing directives. The IP Gateway system owner was involved in the development of DHS NPPD SCG-001 which included consideration of information in the IP Gateway and its predecessor system, the Linked Encrypted Network System. Security classification guides maintained by NPPD are currently undergoing review and evaluation as part of the FY 2017 Fundamental Classification Guidance Review required by EO 13526 and guided by the Information Security Oversight Office and the DHS Office of Security, Administrative Security Division, Administrative Security Policy & Implementation Branch.

- IP officials produced comprehensive procedural manuals pertaining to Protected Critical Infrastructure Information (PCII) and Chemical-terrorism Vulnerability Information (CVI) information contained in the IP Gateway that provide users with requirements, roles, and responsibilities for handling and safeguarding such information. IP officials produced these procedural manuals for PCII and CVI information pursuant to the Critical Infrastructure Information Act and Section 550 of Public Law 109-295 respectively, as well as the implementing regulations.

- Immediately after the whistleblower expressed to her managers concerns about the security of the IP Gateway, IP officials sought guidance and assistance from the DHS Chief Security Officer and Argonne National Laboratory (ANL). The DHS Chief Security Officer provided IP officials with an IP Gateway Classification Review to assist in making an original classification authority decision and ANL provided IP officials with a discussion paper on the IP Gateway Assessment Data. Neither entity concluded that the IP Gateway was improperly secured.

- On May 22, 2015, the Assistant Secretary of the Office of Infrastructure Protection documented a decision that the IP Gateway and its associated products do not require classification and that existing PCII, CVI, and For Official Use Only (FOUO) control systems provide sufficient and adequate protections. According to Office of Infrastructure Protection officials and records, this decision was based on consideration of several factors, including: the Infrastructure Protection mission; review and guidance provided by the DHS Office of Security; a review of IP Gateway products; consideration of existing protections (e.g., PCII, CVI, FOUO); consultation with owners of similar systems; consultation with DHS stakeholders; and the sensitivity, value, utility, and provenance of the information.

The IP Gateway meets information security standards established for high impact information systems as established by NIST and the DHS 4300A Sensitive Systems Handbook. The NPPD Chief Information Officer (CIO), through the Chief Information Security Officer (CISO), provided an authority to operate for IP Gateway, based, in part, on results of a system security assessment and a determination that risk to agency operations, assets, and individuals is acceptable to NPPD. Additionally, a Federal Information Security Modernization Act (FISMA) scorecard shows scores ranging from 95-100% for compliance with information security standards.

Lastly, IP officials took steps to ensure the security of information accessed through the IP Gateway when it expanded access to state and local government users. The expansion began with a pilot program of a small number of SLTT representatives before being widely implemented. IP Gateway is built to provide means to limit and restrict access to data as necessary. For example, access can be limited within state boundaries and can be further restricted down to zip codes, counties, etc. Also, each potential user's application is reviewed by an IP Gateway administrator to vet and grant access to information

The IP Gateway is an unclassified, DHS IT system, meeting DHS and NIST information security standards. The system owner manages the IP Gateway under a documented authority to operate issued by the NPPD Chief Information Officer. The NPPD Office of Privacy maintains an inventory of all the IP Gateway's applications and works with IP officials on a continual basis to review and assess new applications, as well as changes to existing applications, to ensure that proper privacy compliance documentation is in place and that all privacy risks are being managed appropriately. The IP Gateway uses a number of continuous monitoring tools to maintain a secure baseline and to prevent unauthorized access, including centralized logging and vulnerability scanning tools. The likelihood of unauthorized access is mitigated through technical controls including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and other security measures. All implemented controls meet federal and DHS requirements governing information assurance. Finally, the IP Gateway is also separately monitored by the National Cybersecurity and Communications Integration Center (NCCIC) using integrated intrusion detection devices.

Relevant Authorities, Regulations, and Policies

- Executive Order (EO)13526, Classified National Security Information

  EO 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Original classification of information must meet all the conditions under section 1.1(a) of the EO:

  - An original classification authority is classifying the information;
  - The information is owned by, produced by or for, or is under the control of the United States Government;

- The information falls within one or more of the categories of information listed in section 1.4 of the EO[2];
- The original classification authority determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Executive Order 13526 also states in 1.1(b) that "If there is significant doubt about the need to classify information, it shall not be classified." The EO defines the phrase *damage to the national security* as "harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information."

- Title 6 Code of Federal Regulations (C.F.R.) Part 27, Subpart D, Section 27.400 Chemical-Terrorism Vulnerability Information

  6 CFR 27.400 governs the maintenance, safeguarding, and disclosure of information and records that constitute Chemical-terrorism Vulnerability Information (CVI). It prescribes duties and procedures for storing, safeguarding, and transmitting CVI, including limiting distribution to persons with a need to know and clearing marking the CVI with specific language and also distribution limitation language.

- Title 6 C.F.R. Part 29, Protected Critical Infrastructure Information

  6 C.F.R. 29 governs the receipt, care, and storage of Critical Infrastructure Information (CII) when it is voluntarily submitted to DHS. It provides procedures for the receipt, validation, handling, storage, proper marking and use of information as Protected CII (PCII) and the safeguarding and maintenance of the confidentiality of such information, appropriate sharing of such information with State and local governments.

- DHS Delegation 8100, Rev. No. 5, Delegation of Original Classification Authority

  Two officials within NPPD have been delegated original classification authority. The DHS Secretary has delegated original classification authority, through DHS Delegation 8100, Revision Number 05, issued June 4, 2010, to the NPPD Undersecretary to classify national security information at the Top Secret, Secret, and Confidential levels. The

[2] Section 1.4 (G) of Executive Order 13526 pertains to "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security."

NPPD Assistant Secretary of the Office of Infrastructure Protection is also delegated authority to classify national security information at the Secret and Confidential levels.

- DHS 4300A Sensitive Systems Handbook

This Handbook serves as the foundation on which DHS Components are to develop, build, and implement their information security programs; it provides specific techniques and procedures for implementing the requirements of the DHS Information Security Program for Sensitive Systems, and for meeting the Program's Baseline Security Requirements (BLSR), which are generated by the DHS information security policies published in DHS Sensitive Systems Policy Directive 4300A. Components must address these BLSRs when developing and maintaining information for their security documents.

This Handbook contains a compilation of DHS Component best practices that adhere to DHS Information Technology (IT) security policies and meet requirements contained in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, and Congressional and Executive mandates.

Examples of NIST standards referenced include NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems; National Institute of Standards and Technology (NIST) Federal Information Processing Standard FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006; and NIST Special Publication (SP) 800-53, Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, with updates as of January 22, 2015.

Findings for each Allegation

Allegation 1: The IICD failed to conduct a damage assessment of the IP Gateway to determine whether the collection of information available through the IP Gateway should be classified, and it failed to adequately assess individual items for classification.

A variety of authorities guide the protection of the information in the IP Gateway. As part of this inquiry, OCS personnel reviewed *Security Classification Guides: A Guide for Writing a DHS Security Classification Guide*, (updated June 2013), a DHS Office of the Chief Security Office guide. This guide outlines the steps for creating a DHS security classification guide and provides a template to assist users in development. The guide supports IP's decision not to classify the information at issue. For example, the guide indicates that simply because information falls within one of the categories of information defined in EO 13526, Section 1.4, "does not mean the information should automatically be classified." The guide states further that "The decision to classify or not is at the discretion of the OCA based on a determination it's unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security."

The guide also requires that all security classification guides undergo review and evaluation at least once every five years. DHS SCG NPPD-001, issued and approved by the original classification authority (former Assistant Secretary of NPPD's Office of Infrastructure Protection) on December 2, 2010 is currently undergoing review and evaluation as part of the FY 2017 Fundamental Classification Guidance Review (FCGR) required by EO 13526. A review of March 17, 2016 memorandum from the Director, Information Security Oversight Office (ISOO) to Senor Agency Officials designated under section 5.4(d) of EO 13526, states in part that:

> "The goal of the FCGR is to ensure agency classification guidance authorizes classification only in those specific instances necessary to protect national security. A reasonable outcome of the review overall, though not necessarily in the case of each program or guide, is to expect a reduction in classification activity across government."

The ISOO memorandum articulates the objective of the FCGR as ensuring "classification guidance is up-to-date and reflects current circumstances. The FCGR aims to ensure current guidance in use at agencies keeps classification to the minimum necessary and supports the declassification of information that no longer requires protection."

In addition to reviewing *Security Classification Guides*, OCS personnel reviewed the *Reducing Overclassification Act of 2010*, as well as two DHS Office of Inspector General reports mandated by the Act. These materials also support IP's decision not to classify the information at issue. The Act requires the DHS Secretary to develop a strategy to prevent the over-classification and promote the sharing of homeland security and other information. Section 2 of the Act contains certain findings of Congress. Four of those findings are included here:

> (1) The National Commission on Terrorist Attacks Upon the United States (commonly known as the ''9/11 Commission'') concluded that security requirements nurture over-classification and excessive compartmentation of information among agencies.
>
> (2) The 9/11 Commission and others have observed that the over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.
>
> (3) Over-classification of information causes considerable confusion regarding what information may be shared with whom, and negatively affects the dissemination of information within the Federal Government and with State, local, and tribal entities, and with the private sector.
>
> (4) Over-classification of information is antithetical to the creation and operation of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

As part of this inquiry, OCS interviewed the Division Director of IP's IICD who stated that he has never conducted a formally written "damage assessment" of the IP Gateway to determine if the collection of information available through the IP Gateway should be classified, nor is he aware of any damage assessment having been conducted; although, as discussed below a series of steps were taken to protect the information in the IP Gateway. The Division Director stated that the IP Gateway is an unclassified system. He does not believe any of the information contained in the IP Gateway, if compromised, would potentially damage national security. In the Division Director's opinion, none of the information found on the IP Gateway can be combined by a user to become classified information because the IP Gateway contains no threat or intelligence information. He continued and stated the majority of the information found on the IP Gateway is private sector proprietary information, which allows the submitter to withdraw their information from DHS and the Protected Critical Infrastructure Information (PCII) program.[3] The Division Director further stated that the majority of information in the IP Gateway is protected under the PCII requirements.

The Division Director also stated that the IP Gateway contains information protected under the Chemical Facilities Anti-Terrorism Standards (CFATS) as Chemical Security Vulnerability Information (CVI).[4] CVI information is also provided by the private sector, but this information is provided in response to federal regulations. The IP Gateway contains unclassified and FOUO information in the form of reports or studies, as well as open source information including Rich Site Summary feeds pertaining to things like weather and traffic.

Because the IP Gateway is protected as PCII and CVI information, OCS consulted the procedures manuals for PCII and CVI, as well as the PCII implementing regulation, which are discussed below. These materials set forth criteria for protecting the information at issue, and further reflect the standards applied to the IP Gateway.

The *Protected Critical Infrastructure Information Program, Procedures Manual* (April 2009) provides guidance governing PCII and the PCII Program as established by Section 214 of the Critical Infrastructure Information Act of 2002 and Section 29.4(b)(4) of the implementing regulation. The manual contains provisions that guide users, among other things, in the protection of PCII. For example, section 6.1.3, *PCII Program Office Marking Requirements*, instructs users that "PCII commingled with classified information must comply with all marking

[3] The Protected Critical Infrastructure Information Program was created under the Critical Infrastructure Information Act of 2002 to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security. The implementing regulation, 6 CFR Part 29 established procedures for the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the DHS.

[4] Chemical-terrorism Vulnerability Information (CVI) is the information protection regime authorized by Section 550 of Public Law 109-295 to protect from inappropriate public disclosure any information developed or submitted pursuant to Section 550. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. Chemical facilities expect that the information provided to DHS will be protected from public disclosure or misuse. The Department expects individuals in possession of CVI to safeguard it with equal care. Following the requirements in 6 CFR § 27.400 and the guidance in the CVI Procedures Manual will ensure sensitive information about the Nation's high-risk chemical facilities is safeguarded.

requirements of both PCII and the highest level of classification with which it is commingled, as prescribed in Executive Order 12958, as amended, and it's implementing Directives. Additionally, section 8.9, *Derivative Work Products*, contains the same language as previously noted. The manual also contains an appendix titled, *PCII Program, Protected Critical Infrastructure Information Best Practices, Work Products* (June 2008). Section 2 of the appendix addresses classified products derived from and containing PCII. This provision states, "Classified PCII derivative products must be handled and protected in accordance with the safeguarding and handling requirements for **both** PCII and the highest level of classified designation within the product."

OCS personnel also reviewed the *Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information (CVI), Revised Procedural Manual* (September 2008). The stated purpose of the CVI Manual is to:

> "provide guidance on how to identify, handle and safeguard information developed by private and public entities under Section 550 of Public Law 109-295 and its implementing regulations, the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27. Pursuant to CFATS, this information is known as Chemical-terrorism Vulnerability Information, or CVI."

The CVI manual covers topics pertaining to CVI such as definitions of CVI, need-to-know, access to and disclosure of CVI, general handling procedures, policy and procedures, and incident reporting for potential CVI violations. Section 8.2 of the CVI manual addresses marking materials containing CVI and indicates that, in certain circumstances, that the information be treated as classified. The relevant part of section 8.2 states:

> "For paper records containing CVI, as required by 6 CFR § 27.400(f), place the below protective marking on the top of the document and the distribution limitation statement on the bottom of: (1) the outside of any front and back cover, including a binder cover or folder; (2) any title page; and (3) each page of the document.
>
> The protective marking is: Chemical–terrorism Vulnerability Information.
>
> The distribution limitation statement is:
>
> WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 CFR 27.400. Do not disclose to persons without a "need to know" in accordance with 6 CFR § 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR §§ 27.400(h) and (i)."

Section 9.2 of the CVI manual suggests that derivative products containing CVI may become classified because of the sensitivity of the resulting analysis or other information included in the document. "Classification of such products must meet the standards and criteria set forth in

Executive Order 12958, *Classified National Security Information* (as amended), and the requirements established in the *Security Classification Guide for Information Collected Pursuant to Section 550 of Public Law 109-295*, DHS SCG PREP – 003, February 2007." DHS SCG PREP-003 was superseded by DHS SCG NPPD-001, signed by the original classification authority on December 2, 2010. Section 9.2 goes on to add that, "any CVI used in any enforcement proceeding under CFATS must be treated as classified information." The CVI manual also requires use of a front and back cover sheet for any documents containing CVI. This cover sheet includes the same warning as noted above and in section 8.2 of the CVI manual: "In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 CFR §§ 27.400(h) and (i)."

OCS personnel also reviewed relevant Security Classification Guides (SCG).[5] NPPD SCGs cover a wide array of topics to include: National Critical Infrastructure Prioritization Program, Critical Foreign Dependencies Initiative, Buffer Zone Protection Program, Blast/Aircraft Impact and Mitigation Measures. Each SCG is marked UNCLASSIFIED//FOR OFFICIAL USE ONLY. NPPD SCGs provide general guidance on when products containing critical infrastructure and key resources information becomes classified. The reason for classification varies among each SCG; however, information contained among the SCGs is classified pursuant to EO 13526, Section 1.4 (b), (c), (d), (e), (f), and (g). According to one SCG, IP assessments are generally unclassified. More specifically, in all cases the integration of threat, vulnerability and consequence information would not be classified; however, in some cases the specificity or sensitivity of the results would rise to the classified threshold. DHS SCG NPPD-01 states that "any analysis that includes classified intelligence information would retain the original classification and be covered by derivative classification authority."

Upon consulting procedures manuals for PCII and CVI, as well as the PCII implementing regulation OCS continued the interview with the Division Director of IP's IICD. The Division Director is designated as the Information System Owner for the IP Gateway. The complainant notified the Division Director of concerns about the information contained in the IP Gateway on January 5, 2015. The complainant, via e-mail message, raised essentially two primary concerns: 1) "how damaging would a release of the information in the Gateway be" and 2) "the public's perspective and incredulity that we didn't better protect/classify the very information adversaries seek".

In response to the complainant's concerns, and after several discussions among IP leadership, and program personnel, the Assistant Secretary contacted the DHS Chief Security Officer on February 24, 2015 via e-mail and requested an independent classification analysis of the compilation of information contained in the IP Gateway. The Office of Security response was a memorandum, dated April 10, 2015, under the subject heading of *IP Gateway Classification Review*. This memorandum includes summary findings of the classification review and provides a framework and questions for consideration that the Assistant Secretary could use in making a classification decision about the information contained in the IP Gateway. In the memorandum, the Office of Security states that "should the OCA [Original Classification Authority] determine

[5] Each NPPD Security Classification Guide reviewed as part of this inquiry is marked UNCLASSIFIED//FOR OFFICIAL USE ONLY.

that classification is appropriate, OCSO strongly recommends against an approach of classifying by compilation." The memorandum from the OCSO contains a caveat indicating that, due to OCSO's lack of subject matter expertise over what is contained in the IP Gateway, OCSO cannot make a recommendation as to what information should or should not be classified. Therefore, the OCSO notes that they can only assist the Original Classification Authority (i.e., Assistant Secretary) in framing the questions to consider in making a classification decision.

The Division Director indicated that, in addition to the analysis conducted by the Office of Security, Argonne National Laboratory (ANL) produced a report discussing the security of information contained in the IP Gateway.

The ANL report is titled, *Discussion of IP Gateway Assessment Data Access*. The ANL report is not dated; however, the Division Director stated that he believes the report was transmitted to IP via e-mail on or about January 14, 2015. The ANL report is marked in the document header, on each page, with the following caveat: FOR OFFICIAL USE ONLY//FOR INTERNAL IICD USE ONLY. The report's main topic focuses on assessment of data in the IP Gateway to answer what are referred to as three high-level questions. The following is a summary of the ANL report's questions and the respective answer.

1. What does the aggregation of the assessment data from multiple sites within IP Gateway reveal?

The data in the IP Gateway were first collected using a simplified checklist of physical protection survey questions. The data were used to develop classified reports using the Department of Energy (DOE) Security Classification Guide CG-SS-4 pursuant to an April 6, 2004, DOE memorandum applying the SCG to assessments conducted at privately owned facilities. These reports are still maintained in a classified environment. Redacted versions were created in 2005 and 2006; known as the "Green Reports", they were posted to the IP Gateway's predecessor system LENS. The Green Reports are still available on the IP Gateway.

In 2004, DHS issued PCII regulations and guidance. Beginning in 2006, assessments were conducted under PCII protection and housed within LENS. These assessments included physical protection information, but they began to add information about potential threats, as well as mitigation strategies for identified vulnerabilities. These Site Assistance Visit (SAV) and Protective Security Advisor (PSA) reports contained more information on threat and consequence than the current IST-based reports/dashboards.

In late 2008, the Infrastructure Survey Tool (IST) was initiated. From late 2008 until the present, the IST has been used to gather assessment data. Over time, these assessment questionnaires expanded to include more than physical protections, as well as the facility's dependencies on outside resources such as electric power and water. The IST is defined as a security survey rather than a vulnerability assessment. IST data may infer a specific vulnerability from the answer to a particular question. The questions in IST are written as positive protection and resilience measures. This means that a "yes" answer represents and

existing protective measure, while a "no" answer represents a vulnerability. The options for consideration provided in past SAV written reports and in Version 5.0 of the IST also would reveal general, unspecified, and specific vulnerabilities. These sections of the report and IST database have more detailed information concerning facility vulnerabilities than do the yes/no answers to the IST questions.

The current consequence section questions gather information about the general criticality of a facility as a lifeline asset (i.e., utility) or a sole-source provider of service. The economic impact questions use large bins to preclude revealing an owner's proprietary data. Most of the consequence questions would not reveal a specific impact to national security from the loss or degradation of the facility, but merely an acknowledgement that the site may have the potential for impact. Other than the impacted offsite population question, no specific impact information is provided in the answer to the IST questions in this section.

More specific vulnerability and consequence data may be revealed in the IST database comment boxes. Generally, assessors include very little information in comment boxes. DHS and DHS contractor assessors are trained to not include any information concerning impacts on national security within the comment boxes in the IST whether the assessment data are collected as PCII or FOUO. In the Regional Resiliency Assessment Program (RRAP), the comment boxes in the IST were used to gather a broader scope of information about the system or region served by the facility being assessed. Again, assessors are trained to not include any information that would reveal a national security impact, as defined within DOE CG-SS-4 or later under DHS SCG NPPD-01.

Certain types of assessments have written reports generated to summarize the data in the dashboard, provide a more detailed description of the facility, and identify options for consideration; however, they would not necessarily reveal the impact of the loss that a facility would have on national security. Both the dashboards and reports are derivative products created from the PCII or FOUO data collected using the IST tool and would have the same sensitivity as the data. The description may reveal some general impacts due to the loss of the facility; however, assessors are trained to not include in any such description text information that would reveal an impact on national security.

The IST data are used to make a dashboard that displays the facility's answers to each question within the IST. The dashboards show the physical protection, resilience measures, and dependencies compared to other similar facilities, using a calculation based on a relative value formula resulting in two indices. The dashboard could itself reveal vulnerabilities but would not reveal consequences or impact on national security, because no text information is included.

The availability of the database from multiple sites would allow ranking of facilities by vulnerability, but the impact the loss of a given facility would have on national security would not be apparent except in the most general manner. Information in the comment

boxes cannot be data mined to allow a quick ranking based on vulnerabilities or consequences.

2. What is the possible extent to which IP Gateway data could be compromised?

   Only IP Gateway administrator personnel can access the production database; however, the database cannot be downloaded in total. DHS users have access to all assessments, including all sites, all states, and all version/years. They do not have access to the production database. They cannot download the database as a spreadsheet or table. Analysts can only use the database answers by submitting queries to an administrator.

   State users have more limited access. The state administrator determines the access/role provided to state users. State users are limited to assessments collected after 2011. The earlier version contains greater detail when it comes to options for consideration and possible threats. The potential for compromise through a single state user is limited to the level of access granted to the user; the most that can be lost is data for assessments conducted throughout the entire state for assessments conducted after 2001.

3. What protections are in place to prevent compromise of IP Gateway data?

   The IP Gateway is a certified and accredited DHS IT system. The governance rules dictated by the DHS standard are met and enforced. The entire IP Gateway accreditation package is stored in the DHS tool called XACTA (or IACS). This would include the system security plan and the control implementations.

   State administrators are not required to certify or accredit their state systems under the DHS standards. The state systems do not connect directly to the IP Gateway; the only connection to the IP Gateway is via a secure sockets layer-virtual private network connection and internet protocol address for each user (a two-factor authentication).

   All IP Gateway users who are approved for access to the IP Gateway must be PCII certified, be responsible for homeland security duties, and have a valid need-to-know. DHS users must meet DHS suitability requirements. No background checks are currently required for state users, but such a requirement could be imposed pursuant to PCII regulations. Data access and manipulation is limited based on a user role. There is not a mechanism to download the entire database. Reports must be downloaded one at a time. Access to downloaded information is logged; recording when and what information was downloaded, and who downloaded it. When DHS received this OSC referral, access and download tracking records were not reviewed routinely. As part of ongoing enhancements and modification to the IP Gateway since that time, additional processes have been implemented to track IP Gateway activities.

In a second follow-up interview with the Division Director, he provided a May 22, 2015 memorandum signed by the Assistant Secretary of the Office of Infrastructure Protection under the subject of *IP Gateway Classification Decision*. The Division Director indicated that in this

memorandum, the Original Classification Authority (Assistant Secretary, Office of Infrastructure Protection) documented a decision that "the IP Gateway and its associated products do not require classification." The basis for this decision included consultation with owners of similar systems and DHS stakeholders, as well as review of IP Gateway products using the considerations outlined in the April 10, 2015 memorandum from the DHS Office of the Chief Security Officer, (i.e., *IP Gateway Classification Review*). The Assistant Secretary confirmed, via the memorandum, that existing practices are sufficient and adequate to protect the information contained on the IP Gateway. Those protections include "a combination of PCII, CVI, and FOUO control systems."

The Division Director stated that the classification decision was originally made at the inception of the IP Gateway, validated in May 2015, and documented by the original classification authority via memorandum. The rationale used in making the original classification decision documented in the Assistant Secretary's May 22, 2015 memorandum included consideration of the DHS Office of Security's review, as well as the nine questions to consider that were included in the *IP Classification Review* memorandum. The Division Director also stated that the rationale considered the sensitivity, value, utility, and provenance of the information in the IP Gateway. The Assistant Secretary's classification decision memorandum also indicates consideration of the mission of the Office of Infrastructure Protection, and the balancing of information protection with the mission need to disseminate information to a wide audience of stakeholders. The Division Director stated that he was a member of the working group responsible for development of DHS NPPD SCG-001 and that the information contained in the IP Gateway, and its predecessor system the Linked Encrypted Network System (LENS), was considered in the development of the security classification guide.

OCS personnel reviewed e-mail messages exchanged between ANL and the Division Director. Those messages indicate that the information reviewed by ANL had been reviewed for classification. In one particular message dated January 21, 2015 ANL stated that "Argonne staff review the FOUO SAVs for classification." The message indicates further that "a decision was made . . . that SAVs contained vulnerability and options for consideration-providing a forum for possible classifiable inputs. Therefore, it was decided that the FOUO SAVs would be reviewed, but the FOUO ISTs, which only have survey questions and result in only a dashboard, did not need derivative classifier reviews. Note, 91% of the ISTs/SAVs are PCII, the remaining 9% came in as FOUO." ANL "stressed that those FOUO documents or data for which Argonne is responsible have been reviewed for classification."

Allegation 2: IICD failed to ensure that the information security for the IP gateway complies with applicable information security standards for high impact systems.

OCS personnel interviewed employees from the NPPD Office of the Chief Information Office to include the Chief Information Officer and the Chief Information Security Officer. According the NPPD Office of the Chief Information Office, the IP Gateway meets information security standards established for high impact information systems as established by NIST and the DHS 4300A Sensitive Systems Handbook. An authority to operate pertaining to the IP Gateway was issued on July 9, 2015, via memorandum, from the NPPD Chief Information Officer, through the

NPPD Chief Information Security Officer, to the Division Director of IP's IICD (Information System Owner for the IP Gateway). The Chief Information Officer's authority to operate was based, in part, on the results of a system security assessment of the IP Gateway's general support system, its constituent system-level components, and the supporting evidence provided in the security authorization package. The security authorization package consisted of a security plan, security assessment report, and a plan of action and milestones. The authority to operate was issued based on a determination that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable to NPPD. The authority to operate is valid for a period of three years during which time subsequent assessment will need to be conducted in order for the system to maintain its authority to operate.

The Office of the Chief Information Officer also provided OCS personnel with a copy of a DHS Federal Information Security Management Act (FISMA) scorecard. This document identifies the IP Gateway as a high-value asset and mission essential system. The scorecard measures compliance with multiple information security compliance metrics. The IP Gateway results for measures of weakness remediation, hardware, software, configuration management, vulnerability management, anti-phishing/malware management, and indicators of compromise (24-hour monitoring) show ranges of between 95 percent to 100 percent compliance with information security standards.

When OCS personnel interviewed the IICD Division Director, he also referred to the authority to operate pertaining to the IP Gateway that was issued on July 9, 2015, via memorandum, from the NPPD Chief Information Officer. The Division Director stated that, in addition to the authority to operate, the IP Gateway has just under 1000 pages of program and security documentation related to the IP Gateway. IICD performs an annual system test and evaluation of the IP Gateway to confirm and validate the information in the security plan and supporting documentation is accurate. The IP Gateway has extensive ongoing monitoring. System monitoring, for example, tracks internet protocol information such as source of the internet protocol; destination of the internet protocol; version; user access to what type of information; when the user accessed information, both by application and product; restrictions on the amount of data that can be downloaded; flags with automated notification for anomalies; detection and prevention of intrusions; identifying compromised agency information systems; system components; or host computers to permit participating agencies to locate compromised hosts, components, and systems and respond to cyber incidents; ongoing real time system monitoring and analysis of risk, and much more on individual users, organizations, and groups. The IP Gateway is also separately monitored by the National Cybersecurity and Communications Integration Center (NCCIC)[6] using integrated intrusion detection devices.

OCS personnel also reviewed the *Privacy Impact Assessment for the Infrastructure Protection Gateway, DHS/NPPD/PIA-023,* (July 28, 2015), completed by the DHS Chief Privacy Officer. The Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.

[6] The NCCIC shares cyber threat and mitigation information with government, private sector, and academic partners drawing on its operators and analysts while ensuring continuity of national security and emergency preparedness communications. The cybersecurity programs protect Federal networks by providing tools and services to Federal agencies and leading or assisting in the implementation of cross-government cybersecurity initiatives.

The PIA indicates that a security plan had been completed for the IP Gateway, that it received an authority to operate that is effective through July 2018, and that the system has been granted admission into the ongoing authorization program. The PIA also documents that the NPPD Office of Privacy maintains an inventory of all the IP Gateway's applications and works with the system owner on a continual basis to review and assess new applications, as well as changes to existing applications, to ensure that proper privacy compliance documentation is in place and that all privacy risks are being managed appropriately. The PIA also notes that "the IP Gateway uses a number of continuous monitoring tools to maintain a secure baseline and to prevent unauthorized access, including centralized logging and vulnerability scanning tools." The PIA further provides that:

> "The likelihood of unauthorized access is mitigated through technical controls including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and other security measures. All implemented controls meet federal and DHS requirement governing information assurance."

According to the PIA, "users outside the DHS with access to the IP Gateway will not receive privacy training from DHS. However, all DHS users (employees and contractors) undergo DHS privacy training which includes a discussion of the DHS Fair Information Practice Principles (FIPPs) and instruction on handling PII in accordance with FIPPs and DHS privacy policy." All DHS and contractor personnel are required to complete privacy refresher training and security training is also provided to DHS personnel annually.

Allegation 3: IICD failed to ensure the security of information accessed through the IP Gateway when it expanded access to state and local government users without ensuring compliance with information security standards.

The Division Director states that IICD did not fail to ensure the security of information accessed through the IP Gateway when it expanded access to state and local government users. The Division Director reiterated that the IP Gateway has an authority to operate, signed by the NPPD Chief Information Officer on July 9, 2015.

The complainant notified the Division Director of concerns about the information contained in the IP Gateway on January 5, 2015. The complainant expressed concerns, in a general sense, regarding two issues associated with IP's strategy to open IP Gateway information to SLTT partners (i.e., determining need-to-know for SLTT partners and system access controls).

According to the Division Director, in June 2014 a small number of SLTT representatives were part of an IP Gateway pilot to allow SLTT partner access to the IP Gateway. Following the pilot program, in the January/February 2015 timeframe, IICD officially implemented access of the IP Gateway to SLTT partners. The IP Gateway has multiple ways of providing and restricting access to data in the IP Gateway. Federal mission partners have greater access to data and information such as geospatial information and data layers that are viewable in what is called the Map View feature. Data restrictions include the capability to partition state data. This capability was implemented so that state partner access is limited within the user's state boundary,

including access to studies and reports. State-wide data can further be partitioned to include zip codes, jurisdictions, counties, and or any combination of those elements. Additionally, the Division Director stated that not all data fields are available to all users. Data fields like contact information for critical infrastructure assets can be restricted.

The Division Director also indicated that there are three primary roles within the IP Gateway: Administrator, Assessor, and Analyst. The Administrator has the ability to request additional accounts for their state to support adding additional Assessors and Analysts, in addition to having all of the read and write capabilities. The Assessor has the ability to read and write to the IP Gateway. This means they can add security survey information from one of the existing security surveys included within the IP Gateway. The Analyst has only read capability for the IP Gateway. In addition to these role restrictions, other restrictions are placed on the amount of data or information an IP Gateway user can download or upload.

The Division Director stated that SLTT users granted access to the IP Gateway are required to acknowledge the IP Gateway Rules of Behavior and the IP Gateway Terms of Service. The Division Director provided OCS personnel with copies of these documents for review.

The Division Director also enumerated the training required of users granted access to the IP Gateway. These requirements include: PCII training; Background to the IP Gateway; Overview of the Methodology of Infrastructure Survey and Assessments; Scheduling a Survey or Assessment; Understanding Dependencies; Understanding Specific Assets and Areas; Surveying Perimeter Security & Barriers; Surveying Illumination, Parking, and Building Envelope; Surveying Security Activity History & Background; Security Management Profile & Security Force Profile; Entry Controls and Electronic Security Systems; Introduction to State-level Dashboards; Using Map View; Conducting a Rapid Survey; Using the Information Center; Introduction to Event and Incident Tracking; Threat Matrix; State Overview; Documents; Key Contacts; Tracking Special Events; Tracking Domestic Incidents. Those granted the role of Administrator are also required to complete a training module on Managing User Accounts. CVI training is required for those requesting access to CVI information. According to the *Privacy Impact Assessment for the Infrastructure Protection Gateway, DHS/NPPD/PIA-023,* (July 28, 2015), completed by the DHS Chief Privacy Officer, "users outside the DHS with access to the IP Gateway will not receive privacy training from DHS."

Further review of the PIA provides additional information about procedures for granting access to the IP Gateway.

> "Before a user is granted access to the IP Gateway, the IP Gateway Administrator assigned to review the applicant's IP Gateway Account Request Form is responsible for ensuring that the user's access is limited to only the data for which the user has a need-to-know, per PCII data protection requirements. IP Gateway Administrators are responsible for vetting and granting access for requesting homeland security professionals to one of three user roles."

The PIA also expands upon the summary of user roles previously described by the Division Director. According to the PIA:

> "Administrators may view the IP Gateway's entire suite of capabilities, in addition to having the responsibility for managing the accounts of the IP Gateway users who work in their community. Administrators have read and write access to the User Management capability, which allows them to determine a user's level of access and privileges within the IP Gateway. They also have read and write access to the surveys and assessments they have conducted, as well as read-only access to completed visits within their community. They have read-only access to critical infrastructure data for their community throughout a series of other IP Gateway tools, as well as read and write access to planning capabilities."
>
> "Assessors conduct critical infrastructure site surveys and assessments. Assessors have read and write access to the surveys and assessments they have conducted, as well as read-only access to completed visits within their community. They also have read-only access to critical infrastructure data related to their community through a variety of IP Gateway tools."
>
> "Analysts are responsible for accessing and analyzing IP Gateway data. Analysts have read-only access to completed surveys and assessments within their community. They also have read-only access to critical infrastructure data related to their community through a variety of IP Gateway tools."

OCS personnel reviewed the *Protected Critical Infrastructure Information Program, Procedures Manual* (April 2009) provided by the Division Director for relevant sections related to this particular allegation. The implementing regulation for PCII required IICD to establish procedures to ensure that all personnel who work with PCII understand and implement certain policy and procedural requirements for receipt, handling, and safeguarding PCII in order to comply with the requirement of the Critical Infrastructure Information Act and the implementing regulation. Section 2.1 of the manual outlines the responsibilities of the PCII Officer: "Each Federal, State, and local government entity electing to participate in the PCII Program must have a PCII Officer who is responsible for ensuring that PCII received by that entity is used, safeguarded, stored, and disseminated in accordance with the requirements set forth in the CII Act, the Regulation, and all other guidance promulgated by the PCII PM."