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

Homeland Security

February 3, 2017

MEMORANDUM FOR THE SENIOR OFFICIAL PERFORMING THE DUTIES OF THE UNDER SECRETARY

FROM: Mark Smythers
Director
Office of Compliance and Security

SUBJECT: **Office of Special Counsel File No. DI-15-1969; Supplemental Report**

Executive Summary

On March 21, 2016, the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Compliance and Security (OCS), received a whistleblower complaint referral from the Office of Special Counsel (OSC). The complaint alleged that NPPD failed to adequately secure critical infrastructure information in the IP Gateway system. NPPD OCS then conducted an investigation and submitted a report to OSC. Subsequently, on December 12, 2016, OSC followed-up with a request for additional information in the form of 21 questions. After both the initial and supplemental investigation, NPPD finds little evidence to corroborate the whistleblower's allegations and provides the report and this supplemental report as a collective response.

For this supplemental report, OCS interviewed additional persons and reviewed e-mail records and other documents obtained in the investigation. OCS interviewed the following additional persons:

- NPPD, Assistant Secretary, Office of Infrastructure Protection (Original Classification Authority);
- NPPD, IP Infrastructure Information Collection Division, Information System Security Manager (IP Gateway);
- NPPD, IP, Chief Enterprise Architecture (IP Gateway); and
- DHS, Chief, Administrative Security Division, Office of the Chief Security Officer.

OCS also reviewed the security authorization package for the IP Gateway and documents related to the DHS information security policy framework. As part of the investigation that culminated in OCS's November 7, 2016 report, OSC interviewed eight individuals, including the whistleblower, and reviewed email records, DHS and National Institute of Standards and Technology policies and guidance pertaining to information security, relevant DHS classification guides, Executive Orders, and various OIG reports.

For the sake of keeping this supplemental report concise and easy to follow, the report provides answers to the twenty-one questions provided by OSC. Please refer to the original report for more details and background on the allegations, investigation, and findings. NPPD OCS's findings, including findings from the initial investigation and the answers provided in this supplement, are as follows:

Allegation #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.

Response #1

This allegation is partially substantiated. It is factually accurate that NPPD did not perform a "damage assessment" of the IP Gateway. The allegation that NPPD failed to assess and determine whether information collected by the IP Gateway should be classified, however, was not substantiated.

Although no damage assessment was performed, there is no statutory, regulatory, or policy requirement to perform damage assessments for unclassified information.

The Assistant Secretary for Infrastructure Protection confirmed, in a May, 2015 memo, that IP Gateway and its associated products do not require classification. This determination was based on a review conducted by the DHS Chief Security Officer which confirmed that existing practices are sufficient and PCII, CVI, and FOUO control systems are adequate. Additionally, the Chief Security Officer strongly recommended against an approach of classifying by compilation.

IP Gateway was purposely designed as an unclassified system and there are many security controls in place. The protection of the unclassified information found in the system is governed by the requirements for Protected Critical Infrastructure Information (PCII), Chemical-Terrorism Vulnerability Information (CVII), and For Official Use Only (FOUO) information. For users who have permission to enter open text, there are layers of controls, including training and terms of service, initial automated warnings, additional alerts when certain key words are used, and review by derivative classifiers using a DHS security classification guide. Other controls can be found in responses to questions #2 and #4 in the supplemental report.

Allegation #2

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

Response #2

This allegation was not substantiated. An authority to operate for the IP Gateway was most recently issued on July 9, 2015, via memorandum, signed by the NPPD Chief Information Officer. The authority to operate was issued based on a determination that the risk to the agency resulting from the operation of the information system was acceptable to NPPD. This determination is supported by application of DHS and NIST standards and

implementation of minimum security requirements for Federal information systems as documented in the Security Authorization Package.

A review of the IP Gateway Security Authorization Package determined that just under five hundred security controls are documented for the IP Gateway and that these security controls align to each of the seventeen security-related areas identified in FIPS 200, as well as to the high baseline controls included in NIST Special Publication 800-53, Appendix D.

Allegation #3

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

Response #3

This allegation was not substantiated. Adding additional users to the IP Gateway (i.e., SLTT users) did not change the way an authorized user accesses the IP Gateway through encrypted sessions over the Internet using two-factor authentication. These are the same controls that exist if a Federal user accesses the IP Gateway. Information in the IP Gateway is not exposed to unmitigated risk by allowing remote access by SLTT users through external information systems. The risk of adding SLTT users was discussed with NPPD's Chief Information Security Officer during the conduct of the IP Gateway Security Assessment in 2015. There have been no known compromises of confidentiality, integrity, or availability since opening the IP Gateway to SLTT authorized users. There have been no known compromises to information system security due to non-compliance with DHS and NIST information system security standards since opening the IP Gateway to SLTT authorized users.

NPPD mitigates the risk of unauthorized access to the IP Gateway by SLTT users in several ways, including: role-based access control, user vetting and validation procedures, third-party identify verification, data partitioning, acknowledgement of system rules of behavior and terms of service, user training, and just under five hundred security controls documented in the System Security Plan. In FY2017, IP officials plan to deploy greater capability to restrict user access and further partition data. This capability will enable IP Gateway Administrators to limit authorized users (Federal and SLTT) access, via data partitioning, to a smaller set of assets, even down to a single asset.

1. ***Why did IP not conduct and document a "damage assessment"? Is it not required?***

There is no statute, law, rule, regulation, or policy requiring the conduct of a damage assessment pertaining to unclassified information. The IP Gateway is an unclassified system that contains unclassified information that is protected pursuant to statutory[1], regulatory[2], and policy[3] requirements governing protection of the individual items of unclassified information compiled in the IP Gateway, that is, Protected Critical Infrastructure Information (PCII), Chemical-Terrorism Vulnerability Information (CVI), and For Official Use Only (FOUO) information. According to 6 CFR Part 29, the compilation of PCII shall be safeguarded and protected in accordance with the provisions of the Critical Infrastructure Information (CII) Act.[4]

[1] Critical Infrastructure Information Act of 2002.
[2] 6 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Final Rule.
[3] Protected Critical Infrastructure Information Program, Procedures Manual, April 2009 and DHS Management Directive 11042.1, Protecting Sensitive But Unclassified For Official Use Only Information, 1/6/2005.
[4] See 6 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Final Rule.

DHS and NPPD officials indicated that the term damage assessment is associated with the action taken in response to the unauthorized disclosure or spill of classified information. DHS administrative security policy defines the term damage assessment as the systematic analysis that determines the impact of a compromise of classified information on the national security of the United States.[5] DHS administrative security policy further guides that a damage assessment is requested if a security inquiry reveals a compromise or a suspected compromise of classified information.[6] Similarly, an unclassified Intelligence Community Directive defines damage assessment as an action in response to the unauthorized disclosure or compromise of classified information.[7]

2. ***Has IP been assessing each individual item for classification?***

The IP Gateway was designed as an unclassified system and remains an unclassified system, and thus each individual item of information is not assessed for classification. However, information is assessed in other ways prior to being loaded onto the IP Gateway. IP officials explained that they validate each submission of voluntarily submitted critical infrastructure information prior to recording the information in the IP Gateway. This validation process entails assessing voluntarily submitted critical infrastructure information to determine if it meets statutory and regulatory requirements for receipt, validation, handling, storage, marking, and use of voluntarily submitted critical infrastructure information.

The inquiry found that, according to an assessment conducted by ANL, as well as information provided by IP officials, the overwhelming majority of the data in the IP Gateway are protected pursuant to PCII protocols. Further, the assessment data containing the FOUO caveat are reviewed for classification using a DHS security classification guide[8] prior to loading the data to the IP Gateway. The Division Director for IICD indicated that a similar percentage of information is collected through a provision of the PCII program called categorical inclusion.[9] Only the PCII Program Office is authorized to validate an IP Gateway submission as PCII. When the information is part of a categorical inclusion, the PCII Program Manager will have previously declared certain subject matter or types of information categorically protected as PCII, and the information will be considered validated as PCII upon receipt by the PCII Program Office. The PCII Procedures Manual outlines a rigorous process that provides oversight of categorical inclusion, to include review and approval by the PCII Program Office.

The Division Director for IICD also indicated that other providers of content to the IP Gateway conduct a separate review and approval of documents prior to FOUO information being added. For example, the IP Gateway contains more than 700 FOUO and unclassified products developed by NPPD's OCIA. Some of these products incorporate data from the IP Gateway. All of these products go through a separate review by OCIA that includes a classification review, using NPPD

[5] DHS Instruction 121-01-011, The Department of Homeland Security Administrative Security Program, 4/25/2011.
[6] Ibid.
[7] Intelligence Community Directive 732, Damage Assessments, June 27, 2014.
[8] DHS Security Classification Guide, DHS NPPD SCG 001 (2010), currently under review.
[9] The PCII Program Procedures Manual defines Categorical Inclusion as: a declaration by the PCII Program Manager that information of a certain subject matter or type, when properly submitted, will be considered validated as PCII upon receipt by the PCII Program Office or any of the Designees. Categorical inclusion programs are negotiated prior to the receipt of submissions.

security classification guides, to ensure the information is releasable, in an unclassified environment, to the widest dissemination possible and to ensure that classified information is not present. Likewise, the IP Protective Security Coordination Division (PSCD) produces studies and reports (e.g., Critical Infrastructure Resiliency Assessments) that are available to authorized users of the IP Gateway. These assessments are reviewed, including classification review, and approved within PSCD prior to placement on the IP Gateway.

The Information Protection Oversight Section within the PCII Program conducts reviews of IP Gateway information to ensure compliance with the standards established through the PCII Final Rule and the PCII Program Procedures Manual. Reviews of products from OCIA and PSCD are conducted each and every time that they develop or update a product. PCII categorical inclusions are reviewed at the time of initial development and when any and all changes to the categorical inclusion are performed.

A review of the IP Data Overview document indicates that a determination was made by IP officials to establish controls to prevent classified information from being placed onto the IP Gateway for tools that allow users to input open text information. For example, the open text areas in an event planning and incident tracking tool provide authorized users with an automated warning that alerts users to ensure that the data they are inputting does not include the types of information designated as classifiable under an NPPD security classification guide.[10] Additionally, if certain key words are found within the open text an additional warning message alerts the user that they have entered text that may include the types of information designated as classifiable under an NPPD security classification guide."[11] The ANL assessment also indicates that certain information in the IP Gateway, due to user ability to add information in the form of open text, is reviewed by derivative classifiers using a DHS security classification guide.[12]

3. ***Has any information within the system been classified?***

The inquiry found that IP officials have not classified any individual pieces of information in the IP Gateway pursuant to Executive Order 13526.

4. ***How are the classification guides applied to the IP Gateway?***

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 in accordance with Executive Order 13526. NPPD security classification guides document precise elements of critical infrastructure information to be protected, including when such information requires classification. IP officials indicated that information from the IP Gateway supports development of various information sharing and analytic products supportive of the DHS mission as required by the Homeland Security Act of 2002. If pieces of information from the IP Gateway are included in such products, the IP Gateway information is required to contain appropriate markings (i.e., PCII, CVI, FOUO). If the product contains classified

[10] IP Data Overview, February 12, 2015.
[11] Ibid, p. 16.
[12] See Argonne National Laboratory discussion paper on IP Gateway Assessment Data and Access, January 14, 2015.

information derived from another source, the product would contain appropriate derivative classification markings consistent with an approved security classification guide and protection of such product would be accomplished via classified systems, not the IP Gateway.

For example, the IP Gateway contains more than 700 FOUO and unclassified products developed by NPPD's Office for Cyber and Infrastructure Analysis (OCIA). Some of these products incorporate data from the IP Gateway. All of these products go through a separate review by OCIA that includes a classification review to ensure the information is releasable, in an unclassified environment, to the widest dissemination possible and to ensure that classified information is not present. Likewise, the Protective Security Coordination Division (PSCD) within IP produces studies and reports (e.g., Resiliency Assessments) that are available to authorized users of the IP Gateway. These assessments are reviewed, including classification review, and approved within PSCD prior to placement on the IP Gateway.

As previously mentioned, a review of the IP Data Overview indicates that a determination was made by IP officials to establish controls to prevent classified information from being placed onto the IP Gateway for tools that allow users to input open text information. For example, the open text areas in an event planning and incident tracking tool provide authorized users with an automated warning that alerts users to ensure that the data they are inputting does not include the types of information designated as classifiable under an NPPD security classification guide.[13] Additionally, if certain key words are found within the open text an additional warning message alerts the user that they have entered text that may include the types of information designated as classifiable under an NPPD security classification guide."[14] The ANL assessment also indicates that certain information in the IP Gateway, due to user ability to add information in the form of open text, is reviewed by derivative classifiers using a DHS security classification guide.[15]

5. ***Are the classification guides that have been used for IP Gateway correct and in accordance with regulations?***

The DHS Chief of Administrative Security, who maintains oversight of information security and security classification guides stated that, to the best of his knowledge, NPPD security classification guides are in compliance with DHS policy and applicable regulations. A separate review of NPPD security classification guides referenced in this inquiry confirmed compliance with 32 CFR Part 2001 in that they contain the minimum prescribed information as required by the regulation[16]:

- Identification of the subject matter;
- Identification of the OCA by name;
- Identification of an agency POC for questions;
- The date of issuance;
- Precise statement of the elements of information to be protected;

[13] IP Data Overview, February 12, 2015.
[14] Ibid, p. 16.
[15] See Argonne National Laboratory discussion paper on IP Gateway Assessment Data and Access, January 14, 2015.
[16] 32 CFR Part 2001.15, Classification Guides.

- Statement as to which classification level applies to each element of information and identification of elements of information that are unclassified;
- Statement/remarks as to special handling caveats;
- Declassification instructions; and
- Statement of reason for classification citing the applicable reason from section 1.4 of Executive Order 13526.

The review of NPPD security classification guides determined that one security classification guide is overdue for review. This security classification guide is undergoing review and update by IP officials and is due for completion NLT June 2017. This particular security classification guide was not overdue when the former employee raised the concern to IP officials in January 2015.[17] Additionally, the review determined that the security classification guides used by NPPD are based on Executive Order 13526, not on a superseded Executive Order.

6. ***Does the IP Gateway contain threat information or not? There appears to be a discrepancy on that issue. See pages 8 and 11.***

The Division Director for IICD initially stated that the IP Gateway does not contain threat information. In a follow-up interview he mentioned that it does contain a threat matrix. The assessment completed by Argonne National Laboratory mentioned the threat matrix, but also noted that the IP Gateway contained information about "possible" or "potential" threats.

The Division Director for IICD clarified that the IP Gateway does not contain current National Intelligence threat information, but rather general categories of threats that might apply to a particular critical infrastructure. This threat matrix includes a range of possible threats[18] that may generally be considered harmful to any of the critical infrastructure sectors. For example, the National Threat Matrix lists common methods of attack such as: active shooter, aircraft, chemical/biological/radiological weapons, cyber-attack, improvised explosive device, and others. Additionally, IP collects general threat information from owners and operators of critical infrastructure, however such information is not available to IP Gateway users because it is compartmented separately within the IP Gateway. Finally, the IP Gateway also contains information that some personnel consider to be threat information, in a general sense, such as traffic, weather, wind, hurricane, seismic, flood, wildfire, and sea level rise. Most of the latter information is integrated into the IP Gateway via RSS feed, is unclassified, and is generally available to the public. This type of general threat information or categories of potential threats seems consistent with the key concept of resilience, as noted in the National Infrastructure Protection Plan, which "includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[19]

These types of general categories of threat information are typically labeled, in DHS guidance documents, as FOUO or are strictly unclassified. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Design Basis Threat Appendix,

[17] See 32 CFR Part 2001.
[18] The DHS Lexicon defines the term *threat* as the indication of potential harm to life, information, operations, the environment and/or property.
[19] NIPP 2013, Partnering for Critical Infrastructure Security and Resilience.

November 2016, contains similar types of general categories of threat information that are marked as FOUO and protected in accordance with DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. [20] The Chemical Facility Anti-Terrorism Standards, Risk-Based Performance Standards Guidance, May 2009, also contains similar categories of threat information and this document is wholly unclassified.[21]

7. ***What entities concluded that the IP Gateway was not improperly secured? How did they make that assessment?***

Although the NPPD Chief Information Officer ultimately made this conclusion when he, as the authorizing official, issued the approved authorization to operate the IP Gateway, other officials were involved in the teamwork that enabled the Chief Information Officer's determination. Other NPPD information security personnel identified as having a role in the Chief Information Officer's determination regarding the IP Gateway included: NPPD Chief Information Security Officer, IP Gateway System Owner, IP Gateway Information Systems Security Manager, IP Gateway Information System Security Officer, and the IP Gateway Security Control Assessor.

The NPPD Chief Information Officer's authorization to operate (a risk management decision) 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.

8. ***Did the May 2015 decision not to classify the IP Gateway include an analysis of whether some information in the system should be classified?***

Analysis was completed initially in 2010 when NPPD was in the process of establishing a security classification guide specific to the protection of critical infrastructure information. NPPD security classification guides identify specific topics of information associated with critical infrastructure protection that meet the standards and criteria for classification and protection in accordance with Executive Order 13526. In developing one particular security classification guide, the compilation of information contained in the IP Gateway was considered. The considerations included what, if any, unclassified information would reveal an additional association or relationship if combined. Based on this consideration, the Original Classification Authority documented, via security classification guide, precise elements of critical infrastructure information to be protected, including when such information required classification.

After fully investigating the whistleblower's concerns regarding the IP Gateway, the Assistant Secretary of IP, an OCA, signed a memorandum dated May 22, 2015, that documents the original classification decision pertaining to information in the IP Gateway. That memorandum states, in

[20] See The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, Design Basis Threat Appendix, November 2016; and DHS Management Directive 11042.1, Protecting Sensitive But Unclassified (For Official Use Only) Information, 1/6/2005.
[21] DHS, Chemical Facility Anti-Terrorism Standards, Risk-Based Performance Standards Guidance, May 2009.

part, that "the IP Gateway and its associated products do not require classification." The OCA decision was based on multiple considerations including: the aforementioned input from DHS OCSO, DOE ANL, DHS OCIO, DHS TSA, the input of subject matter experts, consideration of the mission of the Office of Infrastructure Protection, and the balancing of information protection with the mission requirement to disseminate information to a wide audience of stakeholders.

Based on interviews with IP and DHS officials involved in supporting the Original Classification Authority's decision, the original classification decision included an analysis of the data contained in the IP Gateway and the protection system applied to the data. The analysis is a 19-page document, titled IP Data Overview, that comprehensively outlines the various types of data resident in the IP Gateway, a description of the types of data, identification of the specific module within the IP Gateway where the data resides, the types of questions used to collect the data, and the protection system applicable to the data (i.e., PCII, CVI, FOUO). The analysis indicates that a determination was made, during initial development and periodically throughout the system's existence, by IP officials to establish controls to prevent classified information from being placed onto the IP Gateway, at least for certain tools.

For example, the Division Director for IICD also referred to the previously noted IP Data Overview that was produced in February 2015. A review of this document indicates that a determination was made by IP officials to establish controls to prevent classified information from being placed onto the IP Gateway for tools that allow users to input open text information. For example, the open text areas in an event planning and incident tracking tool provide authorized users with an automated warning that alerts users to ensure that the data they are inputting does not include the types of information designated as classifiable under an NPPD security classification guide.[22] Additionally, if certain key words are found within the open text an additional warning message alerts the user that they have entered text that may include the types of information designated as classifiable under an NPPD security classification guide."[23] Another assessment that supported this fact was the ANL assessment that indicated that certain information in the IP Gateway, due to user ability to add information in the form of open text, is reviewed by derivative classifiers using a DHS security classification guide.[24]

9. ***What other system owners were consulted in reaching the May 2015 decision not to classify?***

According to IP officials, the Original Classification Authority and staff consulted with the System Owner for the Homeland Security Information Network (HSIN)[25] and with DHS Transportation Security Administration (TSA) officials regarding the protection of Sensitive Security Information (SSI).[26]

[22] IP Data Overview, February 12, 2015.
[23] Ibid, p. 16.
[24] See Argonne National Laboratory discussion paper on IP Gateway Assessment Data and Access, January 14, 2015.
[25] HSIN is described as "the trusted network for homeland security mission operators to share Sensitive But Unclassified information. Federal, state, local, tribal, territorial, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to do their jobs."
[26] DHS Management Directive 11056.1, Sensitive Security Information, 11/3/2006.

Similar to the IP Gateway, HSIN is a user-driven, web-based, information-sharing platform that connects homeland security mission partners, including SLTT, to support the DHS mission. HSIN is the information delivery mechanism for the DHS Information Sharing Environment which is mandated by the Intelligence Reform and Terrorism Prevention Act. Unclassified information shared with DHS SLTT partners through HSIN relates to all-hazards and all-threats, law enforcement activities, intelligence activities, man-made disasters and acts of terrorism, and natural disasters. [27]

SSI is a protection system applied to certain transportation security information pursuant to 49 CFR Part 1520. According to the regulation and TSA published information about SSI, SSI is information that, if publicly released, would be detrimental to transportation security. There are similarities between SSI identified in 49 CFR Part 1520.5 and the information contained in the IP Gateway. Some examples of SSI that are similar to IP Gateway information include *vulnerability assessments, critical infrastructure asset information, confidential business information, security training materials, security measures, threat information, security inspections, information circulars, security screening information, identifying information of certain personnel, and systems security information*.[28]

10. ***Who made the original classification decision? Is it documented?***

The Assistant Secretary of IP, an Original Classification Authority, signed a memorandum dated May 22, 2015, that documents the original classification decision pertaining to information in the IP Gateway. That memorandum states, in part, that "the IP Gateway and its associated products do not require classification." The Original Classification Authority 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."

11. ***Did an authority to operate exist before July 9, 2015? If, not, why not? If so, was it documented?***

The Chief of IP's Information Security Section provided a documented history of the IP Gateway's authorizations to operate dating back to April 2009. A summary of IP Gateway authorizations to operate is provided in Table 1. The system name identified in the table as the Linked Encrypted Network System (LENS) is the initial system name given to what is now the IP Gateway.

Table 1. ***IP Gateway ATO Summary***

System Name	ATO Issue Date	Issuing Official	Term of ATO
Linking Encrypted Network System (LENS)	4/14/2009	NPPD CIO	2 Years

[27] Privacy Impact Assessment for the HSIN R3 User Accounts, DHS/OPS/PIA-008, July 25, 2012.
[28] 49 CFR Part 1520.5, Sensitive Security Information.

LENS	9/8/2011	NPPD Authorizing Official	3 Years
IP Gateway	9/6/2014	NPPD Deputy CIO	90 Days
IP Gateway	12/8/2014	NPPD CIO	90 Days
IP Gateway	3/8/2015	NPPD CIO	120 Days
IP Gateway	7/9/2015	NPPD CIO	3 Years

12. ***What are the standards for high impact systems and how does the IP Gateway fulfill each requirement?***

According to IP and NPPD information security officials the standards for information systems vary based on several factors that may include the system purpose, security categorization, changes to the system, risk management decision-making, results of security assessments conducted pursuant to the DHS Security Authorization Process, agency mission, business needs, etc. FIPS 200 specifies a risk-based process for selecting security controls for minimum security requirements, while NIST Special Publication 800-53, Appendix D provides a summary of security control baselines for low, moderate, and high-impact information systems as categorized using the guidance in FIPS 199.

NIST Special Publication 800-53, Appendix D also provides a matrix containing hundreds of system security controls that identify baseline controls tied to the security categorization (confidentiality, integrity, and availability) of the system (i.e., low, moderate, high). The multiple security controls in Appendix D map to the seventeen security-related areas of controls identified in FIPS 200. The seventeen security-related areas of controls identified in FIPS 200 are listed in Table 2:

Table 2. ***FIPS 200 Security-control Areas***

Access Control	Media Protection
Awareness and Training	Physical and Environmental Protection
Audit and Accountability	Planning
Certification, Accreditation, and Security Assessments	Personnel Security
Configuration Management	Risk Assessment
Contingency Planning	System and Services Acquisition
Identification and Authentication	System and Communications Protection
Incident Response	System and Information Integrity
Maintenance	

According to FIPS 200, for high-impact systems, organizations must employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 (Appendix D). NIST Special Publication 800-53 controls are included in DHS IACS and are used in the DHS security authorization process which manages the risk for DHS IT systems (e.g., IP Gateway). To ensure a cost-effective, risk-based approach to achieving adequate security across the organization, security control baseline tailoring activities must be coordinated with and approved by Chief Information Officers, Information Security personnel, and Agency

Authorizing Officials.[29] IP officials stated that NPPD achieved the security control baseline tailoring activities for the IP Gateway by following the DHS Security Authorization process which included coordination with and approval by the NPPD Chief Information Officer, Information Security personnel, and Agency Authorizing Officials.[30]

The risk decision made by the NPPD Chief Information Officer in July 2015 when he issued the signed memorandum giving the IP Gateway System Owner the authorization to operate was based, in part, on the information security team's assessments of the IP Gateway. In conducting these assessments, NPPD information security officials stated that they followed the processes contained in a framework of DHS policy that incorporates NIST security and privacy controls for Federal information systems and organizations. This policy framework includes, but is not limited to the following, and is used within DHS to manage risk associated with the operation of information systems:

- DHS Management Directive 140-01, Information Technology Security Program, July 2014;
- DHS Sensitive Systems Policy Directive 4300A, Version 12, February 2016;
- DHS 4300A Sensitive Systems Handbook, Version 12, November 2015;
- DHS Security Authorization Process Guide, Version 11.1, March 2016;
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems;
- NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

After following the processes outlined in the above policy framework, NPPD information system security personnel determined which standards applied to the IP Gateway by developing a Security Authorization Package. The IP Gateway security authorization package documents how the IP Gateway implements the minimum security requirements for Federal information systems. According to the Chief of IP's Information Security section, the current IP Gateway authorization to operate is supported by the documentation contained in the security authorization package. The security authorization package consists of a System Security Plan, Security Assessment Report, Plan of Actions and Milestones, and the Authorization to Operate memorandum. The IP Gateway information systems security team produced the security authorization package in accordance with DHS Information Technology Security policies and by following the DHS Security Authorization Process Guide, all of which incorporate NIST standards.

According to IP officials, the System Security Plan provides an overview of security requirements for IP Gateway and describes controls in place or planned for implementation to provide a level of security appropriate for the information processed. The System Security Plan resulted from a risk

[29] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*
[30] Security authorization involves comprehensive testing and evaluation of security features (also known as controls) of an information system (DHS Security Authorization Process Guide, Version 11.1, March 16, 2015).

assessment of the IP Gateway that took place between April-May 2015. According to multiple IP officials, the System Security Plan for the IP Gateway is updated annually, most recently in December 2016, and identifies just under five hundred security controls, from among the seventeen security-related areas found in FIPS 200 and Appendix F of NIST Special Publication 800-53. The System Security Plan also documents how IP system security personnel ensure that IP Gateway fulfills each requirement.

13. ***How does IP Gateway meet the information security standards? What measures have been implemented to ensure security?***

The IP Gateway security authorization package documents how the IP Gateway implements the minimum security requirements for Federal information systems. According to the Chief of IP's Information Security Section, the current IP Gateway authorization to operate is supported by the documentation contained in the security authorization package. The security authorization package consists of a System Security Plan, Security Assessment Report, Plan of Actions and Milestones, and Authorization to Operate. The IP Gateway information systems security team produced the security authorization package in accordance with DHS Information Technology Security policies and by following the DHS Security Authorization Process Guide, all of which incorporate NIST standards.

The System Security Plan provides an overview of security requirements for IP Gateway and describes controls in place or planned for implementation to provide a level of security appropriate for the information processed. The System Security Plan resulted from a risk assessment of the IP Gateway that took place between April-May 2015. The System Security Plan for the IP Gateway is updated annually, most recently in December 2016, and identifies just under five hundred security controls, from among the seventeen security-related areas found in FIPS 200 and Appendix F of NIST Special Publication 800-53. The System Security Plan also documents how IP system security personnel ensure that IP Gateway fulfills each requirement.

According to multiple NPPD information system security officials, the System Security Plan is a living document which is updated annually or when changes occur to the security posture of the IP Gateway. Updates to the IP Gateway System Security Plan are documented in IACS and will be reviewed and approved during system reauthorization pursuant to DHS 4300A and the DHS Security Authorization Process.

Our review of the IP Gateway System Security Plan determined that hundreds of security controls are documented for the IP Gateway and that these security controls align to each of the seventeen security-related areas identified in FIPS 200, as well as to the high baseline controls included in NIST Special Publication 800-53, Appendix D. For example, the System Security Plan documents more than forty security controls for the *Access Control* security-related area found in FIPS 200 and NIST Special Publication 800-53, Appendix D.

The System Security Plan also contains enhanced controls required pursuant to DHS 4300A. IP Information System Security officials stated that, if security control enhancements outside of DHS 4300A and NIST 800-53 are deemed necessary to manage risk, IP officials such as the IP Gateway System Owner can implement additional security controls. In addition, the IP Gateway System

Owner also has the authority to recommend risk acceptance for security controls not implemented after a review of costs and benefits of the security controls.

The Security Assessment Report consists of the system Risk Assessment, Security Assessment Plan, and Contingency Plan Test. The Security Assessment Report includes information derived from an evaluation of security controls identified in the System Security Plan and articulates residual risk associated with the system. The Security Assessment Report includes recommendations for correcting any weaknesses or deficiencies in the implemented security controls. The Security Assessment Report states that just under five-hundred security controls are implemented on the IP Gateway. Of the security controls that require a plan of actions and milestones to mitigate residual risk, none present a high risk to the system. According to the Chief of IP's Information Security Section there are currently ten plans of action and milestones that remain open and in various stages of completion.

After evaluating the results of the security assessment, the Security Control Assessor recommended that the Authorizing Official (i.e., NPPD Chief Information Officer) issue an authorization to operate for the IP Gateway based on a determination that implemented security controls represent an acceptable risk to the organization. The Security Assessment Report was approved in 2015 within IACS by the NPPD Chief Information Security Officer as part of the DHS Security Authorization Process.[31]

14. ***The report states that system can limit access but does it limit access? If it does, explain how the access is limited.***

DHS has well-established processes (i.e., previously discussed framework of DHS policy that incorporates NIST security and privacy controls for Federal information systems and organizations) to enhance information security and minimize possibilities for unauthorized access. The IP Gateway System Security Plan documents more than forty security controls within the security-related area of *Access Control* that map to DHS 4300A and NIST Special Publication 800-53.

NPPD mitigates the risk of unauthorized access to IP Gateway through a role-based access control process.[32] The role-based users include Administrators, Assessors, and Analysts. According to the IP Chief Enterprise Architect, the State Administrator grants access to the individuals in their State. As articulated in the IP Gateway Terms of Service, "Access to the IP Gateway is gained through the User Registration process. State, territorial or tribal homeland security authorities will designate Administrators who will be charged with managing and administering the use of the IP Gateway within their respective State, territory, or tribal locality. These Administrators are responsible for ensuring users of the IP Gateway supporting their area of responsibility have a valid need-to-know to access the IP Gateway technologies."[33]

Administrators (PCII Program Office Administrators and State Administrators) vet all potential users to ensure they possess a valid need-to-know, that the need-to-know derives from the conduct of homeland security duties, and to ensure that access is limited to only the information necessary

[31] See IP Gateway, Security Assessment Report (FOUO), June 30, 2015.
[32] Ibid.
[33] DHS, The Infrastructure Protection Gateway Terms of Service Agreement

to carry out assigned homeland security duties. Several IP officials also provided information that, before accessing PCII information in the IP Gateway, an authorized SLTT user must meet certain standard requirements:

- Be an Individual Employee/Contractor for a Federal, State, or Local Government;
- Be assigned Homeland Security Duties;
- Complete PCII Training;
- Sign a Non-Disclosure Agreement (Non-Federal Only);
- Be Certified by the PCII Program Office (Contractors Only); and
- Have a Valid Need-To-Know.

Data partitioning is accomplished by Administrators based on geography (e.g., state, county, city, zip code) as a means to ensure that users only have access to information based on their need-to-know and their specific homeland security duties. For SLTT users, their particular State Administrator determines access and data partitioning based on need-to-know and specific duties related to homeland security. IP officials explained that, in the future, they will deploy greater capability to restrict user access and further partition data. The IP Chief Enterprise Architect is currently overseeing this IP Gateway project. The enhancements are planned for deployment in FY2017. The further restrictions will enable IP Gateway Administrators to limit authorized users (Federal and SLTT) access, via data partitioning, to a smaller set of assets, even down to a single asset, within their authorized geographic boundary.

Prior to accessing the IP Gateway, authorized users must also acknowledge the IP Gateway rules of behavior and terms of service. These documents, in addition to completion of PCII training, inform authorized users of their responsibilities for information security and data protection, as well as DHS policies that they must adhere to when accessing sensitive but unclassified information via IP Gateway, (i.e., FOUO, SSI, PCII, and CVI). These documents also inform authorized users that they are not authorized to process or house classified information on the IP Gateway.[34]

15. ***Did the investigators perform an independent review of the security of the system, other than relying on the FISMA scorecard results?***

The team did not conduct an information system control audit of the IP Gateway pursuant to the Federal Information System Controls Audit Manual (2009).

16. ***What are the downloading and uploading limits?***

According to the IP Chief Enterprise Architect, the IP Gateway has security controls in place that monitor the amount of data being uploaded and downloaded by users of the IP Gateway. IP allows an authorized user to upload 50 megabytes of data at a time. The downloading control is set to alert, via automated message to the IP Gateway Helpdesk staffed by PCII Program Office officials, when 20 or more files are downloaded. This control threshold is currently under review due to the fact that the threshold has not been exceeded to date. As an additional security control,

[34] See IP Gateway Terms of Service Agreement and IP Gateway Rules of Behavior.

the IP Gateway collects and maintains log files that capture downloads. IP Gateway system security personnel analyze metrics from the log files to monitor the amount of information that is downloaded. If an authorized user downloads large amounts of data, then the IP Gateway helpdesk is responsible for contacting the user to ascertain the purpose for downloading the information. If the IP Gateway helpdesk personnel determine the download supports a valid reason or need-to-know, the reason is documented. If the IP Gateway helpdesk is unable to validate the reason for the download, then the user account is placed into inactive status until someone from the PCII Program Office is assigned to begin an investigation. The PCII Program Office's investigation will determine the facts associated with the user and the need-to-know, make a determination as to whether the download meets PCII requirements, whether the user account should be re-activated, whether the user should lose access to the IP Gateway, or whether additional training is required of the user.

17. ***What security measures and oversight are in place?(Seems to be asking the same question as #13)***

The System Security Plan for the IP Gateway is updated annually, most recently in December 2016, and identifies just under five hundred security controls, from among the seventeen security-related areas found in FIPS 200 and Appendix F of NIST Special Publication 800-53. The System Security Plan also documents how IP system security personnel ensure that IP Gateway fulfills each requirement.

18. ***Why are SLTT users not subject to background checks?***

The PCII Program does, however, subject SLTT users to a vetting/verification process that begins with the user submitting an IP Gateway Account Request Form and User Acceptance Form. For SLTT users, the State Administrator verifies the requestor's employment by an SLTT agency, that they have a need-to-know, and that they are responsible for homeland security duties. At the same time, the IP Gateway Administrator from the PCII Program Office conducts vetting to determine whether the applicant has completed PCII training.

According to IP officials, a recent addition to this vetting/validation process is a requirement for all SLTT users of the IP Gateway to also obtain an account through HSIN. According to IP officials and the HSIN Privacy Impact Assessment, HSIN relies on a third-party identity verification provider to ensure full and effective validation through identity confirmation. The identity authentication process uses a third-party identity proofing service to that may include information such as the individual's commercial transaction history, mortgage payments, and past addresses. An individual must correctly answer the knowledge-based questions generated by the third-party identity proofing service in order to authenticate his or her identity and enable access to use HSIN.[35] Leveraging this HSIN account process also allows IP to implement two-factor authentication for SLTT users of the IP Gateway. IP officials told us that, SLTT users of the IP Gateway access the system via login and password, they are directed to HSIN to enter their HSIN login and password, HSIN then sends the SLTT user a one-time PIN code which is used as the second factor for authentication into the IP Gateway.

[35] See DHS, Privacy Impact Assessment for the HSIN R3 User Accounts, DHS/OPS/PIA-008, July 25, 2012.

19. ***The Report states that access can be limited. How is it limited? Who decides on the limits?***

IP and SLTT Administrators limit access to the IP Gateway through the aforementioned role-based access control process, user registration vetting and validation, via technical security controls, and through by following the PCII Program Procedures Manual.

NPPD mitigates the risk of unauthorized access to IP Gateway through a role-based access control process. As previously noted, the role-based users include Administrators, Assessors, and Analysts. Administrators (PCII Program Office Administrators and State Administrators) vet all potential users to ensure they possess a valid need-to-know, that the need-to-know derives from the conduct of homeland security duties, and to ensure that access is limited to only the information necessary to carry out assigned homeland security duties. Data partitioning is accomplished by Administrators based on geography (e.g., state, county, city, zip code) as a means to ensure that users only have access to information based on their need-to-know and their specific homeland security duties. For SLTT users, their particular State Administrator determines what is considered to be a valid need-to-know for access to the IP Gateway.

DHS has well-established and comprehensive processes (i.e., previously discussed framework of DHS policy that incorporates NIST security and privacy controls for Federal information systems and organizations) to enhance information security and minimize possibilities for unauthorized access. According to IP Information Security officials, the IP Gateway System Security Plan documents more than forty security controls within the security-related area of *Access Control*. These security controls stem from DHS 4300A and NIST Special Publication 800-53.

IP officials also stated that adding additional users to the IP Gateway (i.e., SLTT users) did not change the way a user accesses the IP Gateway through encrypted sessions over the Internet using two-factor authentication. These are the same controls that exist if a Federal user accesses the IP Gateway. Information in the IP Gateway is not exposed to unmitigated risk by allowing remote access by SLTT users through external information sessions. SLTT users were allowed access to the IP Gateway in approximately 2014 and this risk was discussed, during the conduct of the IP Gateway Security Assessment in 2015, with NPPD's Chief Information Security Officer. Additionally, IP officials indicated that there have been no known compromises of confidentiality, integrity, or availability since opening the IP Gateway to SLTT users. There have been no known compromises to information system security due to non-compliance with DHS and NIST information system security standards since opening the IP Gateway to SLTT users.

Also, as previously noted, IP officials are planning the deployment of new capability within the IP Gateway that will allow Administrators to limit user access to a smaller set of assets or to even one asset within their authorized boundary.

20. ***How does IP control how many SLTT users get access?***

According to IP officials, this control is exercised by the State Administrator with oversight by the PCII Program Office. IP officials stated that there are just over 2,000 total users with access to the

IP Gateway. Of the 2,000 total users, only 1156 are active users as of January 13, 2017 (this number can fluctuate from day-to-day). Forty-one States have a total of 376 authorized users, but only 200 users are active. In addition, 97 State Administrators are authorized to grant access to the IP Gateway, but only 64 are active.

The IP Enterprise Architect stated that the State Administrators are responsible for granting IP Gateway access to SLTT requestors within their respective state. State Administrators also decide how many authorized users from within the state boundary require access to the IP Gateway. In making this decision, State Administrators are bound by PCII Program Procedures Manual, 6 CFR, and all requirements established for the PCII Program. IP officials indicated that they currently cap the number of State Administrators to no more than five per state. IP has not limited the State Administrators to a certain number of authorized users within their respective state boundary.

IP officials stated that participation in IP Gateway and the PCII Program is voluntary. State governments can elect to designate a State Administrator or chose not to participate. When IICD started allowing the SLTT users access to the IP Gateway, letters were sent to all the Homeland Security Advisors requesting the designation of State Administers. Some states elected to not participate. Now, IICD has experienced instances where the current State Administrator has either gone inactive or in one case the individual has retired and he has not been replaced. When an administrator becomes inactive, the access for all of the Assessors and Analysts who report to the inactive State Administrator is also inactivated.

21. ***Is anyone responsible for providing oversight for the SLTT administrators' decisions?***

IP officials exercise oversight through the aforementioned role-based access control process, user registration vetting and validation, and technical security controls. NPPD has implemented more than thirty security controls within the security-related area of *Audit and Accountability* that map to DHS 4300A and NIST Special Publication 800-53.[36] Audit and Accountability security controls, in part, ensure oversight of the activities of authorized users through monitoring, analysis, investigation, and reporting of anomalous system activity.[37] For example, according to several IP officials, the IP Data Overview analysis completed in February 2015, and the IP Gateway System Security Plan, access to sensitive information in IP Gateway is automatically logged. Logged data elements include, but are not limited to, username, the file being accessed, and a timestamp of when the access occurred.[38] IP Gateway also implements security controls that automatically analyze incoming logs and sends alerts to the IP Gateway Program Office security administrators when detecting suspicious activity (e.g., users who attempt unauthorized access) or system problems using pre-defined rules.[39]

As noted above, the Privacy Impact Assessment for the IP Gateway also found that "the IP Gateway uses a number of continuous monitoring tools to maintain a secure baseline and to

[36] See IP Gateway, System Security Plan (FOUO), December 1, 2016.
[37] FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.
[38] See DHS, IP Data Overview, February 12, 2015.
[39] See IP Gateway, System Security Plan (FOUO), December 1, 2016.

prevent unauthorized access, including centralized logging and vulnerability scanning tools." The Privacy Impact Assessment also documents 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 requirements governing information assurance."[40] This information was verified via review of the IP Gateway Security Authorization Package.

[40] DHS Privacy Impact Assessment for the Infrastructure Protection Gateway, DHS/NPPD/PIA-023, July 28, 2015.