Privacy Impact Assessment
for the

Infrastructure Protection Gateway

DHS/NPPD/PIA-023

July 28, 2015

Contact Point
Michael Norman
Director, Infrastructure Information Collection Division
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
703-235-9520

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) maintains the IP Gateway, formerly known as the Linking Encrypted Network System (LENS), a web-based portal that supports the collection, analysis, and dissemination of critical infrastructure information. NPPD conducted this Privacy Impact Assessment (PIA) to analyze and evaluate the privacy impact associated with the collection of personally identifiable information (PII) from individuals who are IP Gateway users or are seeking access to the IP Gateway, as well as on designated points of contact (POC) from NPPD critical infrastructure partners. This PIA replaces the original LENS PIA.

Overview

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) leads the coordinated national effort to protect critical infrastructure[1] from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community. In support of this mission, IP developed the Linking Encrypted Network System (LENS).[2] As the system expanded to encompass numerous applications[3] and tools maintained by IP and other components within NPPD, LENS was renamed as the IP Gateway. The IP Gateway serves as a portal for a variety of users to access numerous critical infrastructure-related data collection, analysis, and response applications.

The majority of the applications on the IP Gateway are accessed by logging in to the main IP Gateway user interface. Access to the IP Gateway is restricted to only federal, state, and local government critical infrastructure mission partners that possess homeland security responsibilities, have a valid "need to know,"[4] and have completed Protected Critical Infrastructure Information (PCII)[5] authorized user training. In the future, IP plans to expand the

[1] Section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. § 5195c(e)) defines critical infrastructure as namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
[2] *See* DHS/NPPD/PIA-022 Linking Encrypted Network System (LENS), *available at* www.dhs.gov/privacy.
[3] When used in this PIA, the term "application" refers to a single capability under the three capability groups (i.e., Data Collection and Web-Based Dashboards, Information Sharing and Training Tools, and Administrative, Management, and Reporting Capabilities) described in the Overview section. The term "application" does not refer to a separate system or sub-system.
[4] A federal government user's "need to know" is determined by whether or not access to the information is necessary in order to perform his or her official duties. For state and local government users, their particular states define what is considered to be a valid "need to know" for access to the IP Gateway.
[5] PCII is a program that protects infrastructure information voluntarily shared with DHS to be used for homeland security purposes. Through the Critical Infrastructure Information Act of 2002, PCII in the Government's hands is protected from disclosure. See Critical Infrastructure Information Act of 2002 available at:

use of the IP Gateway to include tribal and territorial government critical infrastructure mission partners as well.

Individuals may request access to the IP Gateway by completing the IP Gateway Account Request form via the IP Gateway website at https://ipgateway.dhs.gov. The IP Gateway Account Request Form requests various data elements, which differ based on the type of applicant (i.e., federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor) that is requesting access to the IP Gateway.

In addition to the applications describe above, there are a few applications (i.e., the Modified Infrastructure Survey Tool (MIST), the National Counter-IED Capability Analysis Database (NCCAD), and the Protected Critical Infrastructure Information Management System (PCIIMS)) that sit on the IP Gateway infrastructure, but employ their own individual user registration, management, and authentication processes. Although these applications fall within the security boundary of the IP Gateway, they cannot be directly accessed via the IP Gateway's main user interface. These applications are serviced by the individual programs' Help Desk (not the IP Gateway Help Desk) and can provide access to users outside of the IP Gateway's federal, state, and local government community. These additional users may include tribal and territorial government mission partners, private sector entities, state and local law enforcement, first responders, and State Homeland Security Advisors (HSA).[6] The NPPD Office of Privacy maintains separate internal privacy compliance documentation for each of these applications, as appropriate, and therefore they are not the primary focus of this PIA.

IP Gateway Capability Groups

The IP Gateway provides users with access to a number of applications supporting activities such as data collection and management, operational scheduling, report management, and analysis for comprehensive risk assessment, management/mitigation, and contingency planning. For the sake of clarity, we have established three capability groups, which encompass all of the IP Gateway applications based on their business function(s).

Capability Group 1: Data Collection and Web-Based Dashboards

- Examples of applications that fall under this capability group include data collection and web-based dashboards, such as the Infrastructure Survey Tool, which may be

http://www.dhs.gov/sites/default/files/publications/CII-Act_508.pdf. Also *see* DHS/NPPD/PIA-006(a) Protected Critical Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC), *available at*: www.dhs.gov/privacy.

[6] HSAs are part of the Homeland Security Advisory Council (HSAC), which provides advice and recommendations to the Secretary on matters related to homeland security. HSAC comprises leaders from state and local government, first responder communities, the private sector, and academia. *See* "Homeland Security Advisory Council" *available at:* http://www.dhs.gov/homeland-security-advisory-council-0.

used to collect and display data for the Protective Security Advisors (PSA),[7] Sector Specific Agencies (SSA),[8] or the state, local, tribal, and territorial (SLTT) communities. This capability group allows for analysis of performance and review of vulnerabilities of critical infrastructure. The analysis is focused on physical security, cybersecurity, information sharing, protective measures, and internal and external dependencies. The web-based dashboards may also be used to convey, track, manage, and graphically display information collected by the PSAs or through incident reporting.

Capability Group 2: Information Sharing and Training Tools

- Information Sharing and Training Tools provide for the dynamic sharing of data and information sources. For example, various information sharing tools enable critical infrastructure stakeholders to easily access, search, retrieve, visualize, analyze, and export infrastructure data and resources, including counter-IED information, vulnerability and consequence data, and protective measures. Data purview restrictions and access controls are limited by or based on a user's need to know as described in the "IP Gateway Access Controls" section of this PIA. NPPD may also use these tools to provide knowledge management material for designing employee and stakeholder training content.

Capability Group 3: Administrative, Management, and Reporting Capabilities

- Administrative, Management, and Reporting Capabilities can be used to schedule, track, coordinate, and maintain certain tasks. For example, certain applications in this capability group allow for both field personnel and NPPD/IP leadership (e.g., Assistant Secretary, Deputy Assistant Secretary, Division Directors) at headquarters to provide performance management metrics and quickly assess impacts of missions in the field. In addition, the IP Gateway provides the ability to connect personnel at headquarters with personnel in the field who are performing vital functions to protect our critical infrastructure.

[7] PSAs facilitate field activities in coordination with other DHS offices. The PSA Program maintains a robust operational field capability by: conducting assessments of nationally significant critical infrastructure through Enhanced Critical Infrastructure Protection (ECIP) security surveys; site assistance visits and incident response; and providing access to infrastructure security and resilience resources, training, and information.

[8] SSAs are federal departments or agencies designated under Presidential Policy Directive-21 (PPD-21) to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. *See* PPD-21, *Critical Infrastructure Security and Resilience* (February 12, 2013) *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

IP Gateway applications may collect business contact information for users and other POCs. POCs may include, but are not limited to, private sector partners or stakeholders associated with specific infrastructure assets. NPPD may use this information to communicate with facilities in support of its infrastructure protection mission. For example, during an event or incident, such as an attack or natural disaster, NPPD may need to contact facility owners or operators to convey information to help protect his/her infrastructure. The contact information collected from POCs is limited to full name, email address, office phone number, cell phone number, and business address.

The NPPD Office of Privacy maintains an internal inventory of all IP Gateway applications and works with the IP Gateway Program 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.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

IP Gateway is primarily used to collect non-privacy sensitive infrastructure information as authorized by Section 201(d) of the Homeland Security Act.[9] Furthermore, NPPD's PCII program, authorized by the "Critical Infrastructure Information Act,"[10] controls the protection of the majority of the critical infrastructure information collected and maintained within the IP Gateway.

Most recently, PPD-21 *Critical Infrastructure Security and Resilience*,[11] issued in 2013 specifically directed DHS to:

1) In coordination with SSAs and other federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure; and

2) Conduct comprehensive assessments of the vulnerabilities of the nation's critical infrastructure in coordination with SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators. In support of this Directive, DHS/NPPD/IP employs the IP Gateway, which provides federal, state and local government critical infrastructure mission

[9] 6 U.S.C. § 121(d).
[10] 6 U.S.C. § 131 *et seq.*
[11] *See* PPD-21, *Critical Infrastructure Security and Resilience* (February 12, 2013) *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

partners with various data collection, analysis, and response tools in order to enhance critical infrastructure protection.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

NPPD collects PII from individuals for the purpose of granting access to the IP Gateway. This collection is covered by the DHS system of records titled, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[12] NPPD also collects PII to provide customer support to users through the IP Gateway Help Desk. This collection is covered under DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System.[13]

In addition to the collections described above, the IP Gateway may also maintain limited business contact information on critical infrastructure POCs. This information, however, is not filed or retrieved by the individual's PII and therefore is not covered by the Privacy Act. POC information is generally filed and retrieved by the name of a facility or other asset with which the individual is associated.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A system security plan has been completed for the IP Gateway and the IP Gateway has been issued an Authority to Operate (ATO) through July 2018 and has been granted admission into the ongoing authorization program.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

User registration records are maintained in accordance with NARA's General Retention Schedule 3.2 – Information Systems Security Records, and records created through the IP Gateway Help Desk (IT Customer Service Files) are maintained in accordance with NARA's General Retention Schedule 24 – Information Technology Operations and Management Records.

Additionally, NARA Job No. N1-563-08-36 covers the PCII submitted and maintained through the IP Gateway, and NARA Job No. N1-563-04-09 covers the critical infrastructure submissions that do not meet the requirements for PCII.

---

[12] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm

[13] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The IP Gateway is currently going through the PRA approval process. The IP Gateway's PRA package (DHS Docket ID: DHS-2014-0010) includes both the IP Gateway Account Request Form (used for IP Gateway user registration) and the voluntary IP Gateway Customer Satisfaction Survey. This PRA package has not yet received an OMB Control number.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

In order to register for access to the IP Gateway, individuals are required to provide certain information via the online IP Gateway Account Request Form. This form requests various data elements, which differ based on the type of applicant (i.e., federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor) requesting access to the IP Gateway. The information collected by the IP Gateway Account Request Form is outlined below.

All applicants must provide the following information:

- U.S. citizen (yes/no);
- Employee type (federal employee, federal contractor, state government employee, state government contractor, local government employee, or local government contractor);
- Role requested (e.g., Assessor/Analyst);
- First name;
- Last name;
- Middle initial (optional);
- Role in organization;
- Do they hold any regulatory or rulemaking responsibilities (yes/no);
- Work address;

- Work email;
- Work phone number;
- Mobile phone number (optional);
- Does their organization provide annual Cyber Security and Awareness Training (yes/no);
- Organization's Cyber Security Training Date;
- Their need to know (as verified by IP Gateway Administrators described below);
- For which state they are requesting IP Gateway access (applicant may also request to restrict their access to a particular county, city, or zip code within that particular state);
- PCII trained (yes/no);
- PCII certification number; and
- How they plan to use this information (Analysis or CIP Program coordination; incident planning; emergency response; performing assessments; other).

All additional information requested through the IP Gateway Account Request Form is dependent upon the type of employee requesting access:

- *Federal employees:* Must provide their department or agency; component; work supervisor's first and last name, email address and phone number; and their IP Sponsor's[14] first and last name, email address, and phone number.
- *Federal contractors:* Must provide the department or agency they support; component; contractor representative's first and last name, email address and phone number; contracting company's name and address; and their IP Sponsor's first and last name, email address, and phone number.
- *State and local government employees:* Must provide their state government name and agency.
- *State and local government contractors:* Must provide their state government name; the government agency they support; contractor representatives' first and last name, email address, and phone number; and their contracting company's name and address.

[14] Federal government employees and contractors must provide an IP Sponsor's name and contact information in order to register for access to the IP Gateway. This information is collected so that IP Gateway Administrators may contact IP Sponsors to ensure that the requesting Federal Government employee or contractor has a valid need to know for access to the IP Gateway.

Once a federal, state, or local government critical infrastructure mission partner submits his or her IP Gateway Account Request Form, it is electronically sent to an IP Gateway Administrator. IP Gateway Administrators are responsible for vetting potential IP Gateway users' need to know and for managing their level of access to IP Gateway data. These IP Gateway Administrators are located at both the federal and state levels and are responsible for managing the accounts of IP Gateway users who work in their community (i.e., federal, state, or local government users). For example, if an IP Gateway applicant is a Department of Defense (DOD) employee, then an IP Gateway Administrator working within DOD will be assigned to review/vet the applicant's IP Gateway Account Request Form and determine what level of access (e.g., state, county, city, or zip code-wide), if any, the applicant should receive. There is no difference in IP Gateway user roles or access rights between IP Gateway Administrators at the federal-level versus those working at the state-level. For more information regarding the different levels of IP Gateway access and data partitioning, please see Section 8.3 of this PIA. IP Gateway Administrators at the state-level are appointed by state HSAs and are required, as are all IP Gateway Administrators, to take the DHS provided IP Gateway module training to ensure they understand the requirements to establish a valid need to know for state and local government critical infrastructure mission partners.

When a federal, state, or local government critical infrastructure mission partner initially submits his or her IP Gateway Account Request Form, it is automatically sent to an IP Gateway Administrator, working within NPPD/IP, to review whether or not the applicant has completed PCII Authorized User Training. The review of an applicant's PCII Authorized User Training must be performed by IP Gateway Administrators working within NPPD/IP because Administrators are provided with access to the list of PCII Authorized Users maintained through the PCIIMS.[15] In order to receive access to the IP Gateway, all applicants must be PCII Authorized Users because certain surveys and assessments that are conducted using IP Gateway are secured as PCII. If applicants are not PCII Authorized Users, then they will be redirected to PCIIMS in order to take the training before being granted an IP Gateway account. This PCII Authorized User Training covers the consequences of loss or misuse of PCII data, including criminal and administrative penalties.

Upon review of the IP Gateway applicants' PCII training status, the applicants' IP Gateway Account Request Form is automatically submitted to their assigned IP Gateway Administrator for review based on their community (i.e., federal, state, or local government). Currently, only approved DHS/NPPD employees that meet the IP Gateway's access requirements are provided with access to the national view, since DHS/NPPD leads the national effort to protect and enhance the resilience of the nation's critical infrastructure.

[15] *See* DHS/NPPD/PIA-006(a) Protected Critical Infrastructure Information Management System (PCIIMS), *available at* www.dhs.gov/privacy.

If the assigned IP Gateway Administrator determines that the federal, state, or local government critical infrastructure mission partner meets the necessary requirements for access to the IP Gateway, then the applicant is approved for an IP Gateway user account. The IP Gateway system will electronically send the approved user an email with a username and temporary password for access to system.[16] Upon logging into the IP Gateway for the first time, users will be prompted to complete the IP Gateway user training. This training must be completed before full-access to the IP Gateway is permitted because it provides users with a general overview of the system and its various tools and applications.

NPPD may also collect business contact information from critical infrastructure POCs, which is accessible through the IP Gateway. This business contact information is limited to: full name, email address, office phone number, cell phone number, and business address.

Lastly, the IP Gateway provides a Help Desk as an information and assistance resource for troubleshooting problems with the IP Gateway. The IP Gateway Help Desk provides a single point of contact for both internal and external stakeholders and partners for technical questions and assistance on current tools and applications within the IP Gateway. The IP Gateway Help Desk may collect basic contact information from individuals in order to provide customer support via phone or email. This contact information includes the individual's name, work email, and work phone number.

2.2 What are the sources of the information and how is the information collected for the project?

The information maintained in IP Gateway is received directly from the individual to whom it pertains. Sources primarily include: federal employees, federal contractors, state government employees, state government contractors, local government employees, and local government contractors. Critical Infrastructure POC information may be collected directly from the individual, or may be provided by individuals designated to act on behalf of the critical infrastructure facility or private sector entity via other NPPD programs and uploaded to the IP Gateway. Critical infrastructure information maintained on the IP Gateway may come from a variety of sources, but does not include PII.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The IP Gateway may include information collected from publicly available sources for the purpose of completing and verifying basic identifying infrastructure information in submitted

[16] IP Gateway is actively moving toward two-factor authentication for all IP Gateway users.

site records and for developing background reports on infrastructure that will be later visited by NPPD. This collection, however, does not include any PII.

2.4 Discuss how accuracy of the data is ensured.

To ensure accuracy, NPPD/IP collects registration information directly from individuals that have or are seeking access to the IP Gateway. Contact information is collected directly from critical infrastructure POCs or individuals designated to act on behalf of the critical infrastructure facility or private sector entity.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

There are no risks concerning over-collection or collection of inaccurate PII by IP Gateway. IP Gateway only collects business contact information directly from individuals for the limited purposes of registering users for the IP Gateway, providing quality support via the IP Gateway Help Desk, and gathering critical infrastructure POC information.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

NPPD collects PII from federal, state, and local government critical infrastructure mission partners during the IP Gateway registration process so that NPPD can create and manage IP Gateway user roles and accounts. Once users are provided with an IP Gateway account, these individuals may access a number of applications to conduct comprehensive data collection and analysis consistent with their need to know. Specifically, IP Gateway enables federal, state, and local government critical infrastructure mission partners to manage information about the infrastructure in their communities for risk management, infrastructure protection, event planning, and incident response activities.

These user roles determine what data users may access within the IP Gateway.

- Administrator: 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.

- Assessor: 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.
- Analyst: 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.

The IP Gateway Help Desk also collects PII from current and potential IP Gateway users in order to manage IP Gateway user accounts and to provide quality technical support.

Lastly, NPPD uses critical infrastructure POC information in order to facilitate communications with stakeholders related to critical infrastructure security and resilience.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that users may access IP Gateway applications beyond the scope of their missions.

Mitigation: IP Gateway Administrators vet all potential users to ensure they possess a valid need to know for access, and that their access is limited to only the applications necessary for them to perform their homeland security responsibilities. NPPD further mitigates this risk by ensuring that user PII is only accessible to the IP Gateway Administrators who require access to manage system users. Through this role-based access process, NPPD mitigates the risk of unauthorized access to or misuse of PII. This risk is also mitigated by the IP Gateway Disclaimer (see Attachment 3) to which all users of the IP Gateway must consent before logging into the system. This disclaimer dictates how data may be used and warns users that misuse may be punishable by civil or criminal penalties.

The IP Gateway further grants access to federal, state, and local government critical infrastructure mission partners based on location, including state, county, city, and zip code partitioning options. This ensures that each user has access to only the data for which he/she has a need to know in order to perform his/her homeland security responsibilities. For example, a Virginia state user only has access to IP Gateway data for Virginia and will not be able to access any other state's data. This partitioning extends to the entire IP Gateway suite of applications. Currently, only approved DHS/NPPD employees that meet the IP Gateway's access requirements are provided with access to the national view because DHS/NPPD leads the national effort to protect and enhance the resilience of the nation's critical infrastructure.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

NPPD provides Privacy Act Statements to individuals requesting access to the IP Gateway via the IP Gateway Account Request Form (see Attachment 1) and to individuals contacting the IP Gateway Help Desk (see Attachment 2) before they submit any personal information to NPPD.

Additionally, NPPD provides notice through this PIA and through the publication of the DHS/ALL-002 and DHS/ALL-004[17] SORNs.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All PII is submitted on a voluntary basis and, as such, individuals may elect not to participate. An individual's PII is only used for the purposes of registration, IP Gateway Help Desk support, or contacting POCs as necessary. Users of the IP Gateway may request to update or remove their information by contacting the IP Gateway Help Desk. Help Desk staff will coordinate the request with the IP Gateway Program Manager. The Program Manager will work in coordination with the NPPD Office of Privacy to ensure the updates or removal of the requested information is in accordance with DHS policy.

[17] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm; and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

4.3 Privacy Impact Analysis: Related to Notice

There is no risk of inadequate notice. NPPD provides Privacy Act Statements to individuals requesting access to the IP Gateway via the IP Gateway Account Request Form (see Attachment 1) and to individuals contacting the IP Gateway Help Desk (see Attachment 2) before they submit any personal information to NPPD. Notice is also provided via this PIA and the DHS/ALL-002 and DHS/ALL-004 SORNS.[18]

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

User registration records are maintained until the business use ceases, in accordance with NARA's General Retention Schedule 3.2 – Information Systems Security Records.

Records created through the IP Gateway Help Desk (IT Customer Service Files) are maintained for one year after they are superseded or obsolete, in accordance with NARA's General Retention Schedule 24 – Information Technology Operations and Management Records.

Additionally, NPPD has a retention schedule approved by NARA for PCII submitted and maintained through the IP Gateway under NARA Job No. N1-563-08-36. In addition, the NARA approved retention schedule, NARA Job No. N1-563-04-09, covers the critical infrastructure submissions that do not meet the requirements for PCII.

NPPD is currently working on a comprehensive records schedule for all other records generated and maintained by the IP Gateway system.

5.2 Privacy Impact Analysis: Related to Retention

There are minimal risks that IP Gateway will retain PII for a longer time period than is relevant and necessary under its approved records retention schedules. Audits and ongoing vigilance are applied to verify adherence to applicable records retention schedules. In addition, Section 8.0 of this PIA details the security measures used to safeguard IP Gateway information throughout its lifecycle.

[18] *Id*.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

NPPD critical infrastructure POC information and infrastructure-related data is shared through the IP Gateway with DHS employees as well as state and local government critical infrastructure mission partners who possess homeland security responsibilities, have a valid need to know, and have completed PCII Authorized User Training.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

NPPD does not share any Privacy Act-covered information outside of DHS from the IP Gateway. NPPD collects PII from individuals for the purpose of granting access to the IP Gateway and to provide customer support to users through the IP Gateway Help Desk. These information collections are covered by the DHS/ALL-002 and DHS/ALL-004[19] SORNs and are not shared outside of DHS.

However, IP Gateway also maintains limited business contact information on critical infrastructure POCs. As noted in Section 1.2, this information is not filed or retrieved by the individual's PII and therefore is not covered by the Privacy Act. POC information is generally filed and retrieved by the name of a facility or other asset with which the individual is associated.. This critical infrastructure POC information is the only PII shared outside of NPPD via the IP Gateway with DHS employees as well as state and local government critical infrastructure mission partners who possess homeland security responsibilities, have a valid need to know, and have completed PCII Authorized User Training.

[19] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm; and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

6.3 Does the project place limitations on re-dissemination?

User PII collected for IP Gateway registration purposes cannot be re-disseminated outside of NPPD because the information is collected for the sole purpose of granting access to the IP Gateway.

Some PII associated with NPPD critical infrastructure POCs is intertwined with PCII contained within the IP Gateway. Re-dissemination limitations are consistent with the safeguarding and handling requirements of PCII, which is only shared with PCII Authorized Users that possess a need to know. All other data within the IP Gateway is, at most, Sensitive but Unclassified (SBU) and, as such, is only to be shared with other federal, state, or local entities that possess a need to know.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The IP Gateway audits all user access to its data. As such, a record is maintained, including the name of the user, the date of access, and the data accessed anytime a user accesses or downloads data from the IP Gateway.

NPPD does not share any Privacy Act-covered information outside of DHS from the IP Gateway.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that POC information maintained on the IP Gateway will be shared with individuals that do not possess a need to know.

Mitigation: NPPD mitigates this risk by having IP Gateway Administrators vet potential IP Gateway users prior to access being granted. Toensure that all IP Gateway users possess a valid need to know for access to the POC information maintained on the IP Gateway.

This risk is further mitigated by IP Gateway Administrators limiting users' system access to only the data for which the users have a need to know in order to perform his/her homeland security responsibilities, per PCII data protection requirements. To do this, IP Gateway Administrators assign user roles and partition data based on location. As explained in the "IP Gateway User Roles and Access Controls" section of this PIA, the IP Gateway system user roles (e.g., Administrator, Assessor, or Analyst) determine which applications a user may view within the IP Gateway. Meanwhile, by partitioning data, IP Gateway Administrators can limit federal, state and local government users' access based on their location, to include state, county, city, and zip code partitioning options. As a result, IP Gateway users do not have access to any PII for which they do not possess a need to know This risk is also mitigated by the IP Gateway Disclaimer (see Attachment 3) to which all users of the IP Gateway are required consent to before logging into the system. This disclaimer dictates how data from the system may be used

and warns users that misuse may be punishable by civil or criminal penalties.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

IP Gateway users are able to access their PII via the account management tool or by contacting the IP Gateway Help Desk.

Critical infrastructure POCs also do not have direct access to their information through the IP Gateway. However, POCs have an ongoing relationship with NPPD and can access and correct information that was voluntarily provided to the agency. For example, a POC may choose to contact NPPD to ensure that information on his/her facility, including his/her contact information, is accurate.

Lastly, all individuals may also request access to information about themselves by submitting a Freedom of Information Act (FOIA) or Privacy Act (PA) request to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. Individuals may obtain directions on how to submit a FOIA or PA request at http://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homeland-security.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

IP Gateway users may update their contact information via the account management tool or by contacting the IP Gateway Help Desk. POCs may update erroneous information by making a request to the NPPD component that collected the information from them. Instructions on how to correct inaccurate or erroneous information are provided in this PIA and through guidance issued by the NPPD program office.

Users may also write to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have inaccurate or erroneous PII corrected.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures to correct information through this PIA and the

DHS/ALL-002 and DHS/ALL-004 SORNs.[20] Users may also contact the IP Gateway Help Desk during normal business hours. The Help Desk contact information is readily available on the IP Gateway log-in screen.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may be unaware of or not understand their redress options.

Mitigation: Most PII maintained within the IP Gateway pertains to IP Gateway users, in which case, those users have the ability to access and correct their data via the account management tool or by contacting the IP Gateway Help Desk. Although POCs do not have direct access to information, most POCs can update or correct their data through ongoing working relationships with NPPD. Redress will be provided as described above in sections 7.1-7.2. Notice of redress procedures are also provided in the DHS/ALL-002 and DHS/ALL-004 SORNs.[21] Contact information for the IP Gateway Help Desk is readily available on the IP Gateway log-in screen.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

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 IP Gateway has also been subject to multiple audits by the Government Accountability Office (GAO) and the DHS Office of Inspector General. In addition, DHS policy requires that systems implement auditing at the user level and regularly analyze audit logs to determine misuse or abuse. 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.

The NPPD Office of Privacy maintains an internal inventory of all the IP Gateway's applications and works with the IP Gateway Program on a continual basis to review and assess

[20] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-11-25/html/E8-28053.htm; and DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792, (November 27, 2012), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.
[21] *Id*.

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.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Users outside of 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 instructions on handling PII in accordance with FIPPs and DHS privacy policy. Additionally, all DHS and contractor personnel must complete annual privacy refresher training to retain system access. Security training is also provided to DHS personnel on an annual basis, which helps to maintain awareness for safeguarding PII. DHS reports on employees and contractors who receive IT security and privacy training as required by the Federal Information Security Management Act (FISMA) of 2002.

In addition, certain information maintained in the IP Gateway is considered PCII. As a result, all IP Gateway users are required to take PCII Authorized User Training before they are granted access to the IP Gateway. This training provides IP Gateway users with an understanding of proper handling and safeguarding techniques for PCII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

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 (Administrator, Assessor, or Analyst as described in Section 3.1). Additionally, DHS has well-established and comprehensive processes to enhance information security and minimize possibilities for unauthorized access. DHS personnel adhere to internal information security policies. In addition, robust auditing measures and technical safeguards will help monitor unauthorized access and attempted access. To reduce the risk of a data breach, proactive monitoring of logs will identify potential incidents as early as possible, and audit trails will be maintained to facilitate investigation of incidents in accordance with DHS Privacy Incident Handling Guidance. Regularly scheduled risk assessments will be performed on the security controls to identify potential vulnerabilities, including technical, managerial, and physical security access.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing agreements are developed by the program manager and the system owner in coordination with the IP Data Governance Board and NPPD/IP Privacy Analyst. In addition, the NPPD Senior Privacy Officer and counsel review agreements, access, MOUs, and uses of information, as appropriate.

Responsible Officials

Michael Norman
Director, Infrastructure Information Collection Division
Office of Infrastructure Protection, National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

ATTACHMENT 1

IP Gateway Privacy Act Statement

Authority: 44 U.S.C. § 3101 and 44 U.S.C. § 3534 authorize the collection of this information.

Purpose: DHS will use this information to create and manage your user account and grant access to the Infrastructure Protection (IP) Gateway.

Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70792.

Disclosure: Furnishing this information is voluntary; however failure to provide the information requested may delay or prevent DHS from processing your access request.

ATTACHMENT 2

IP Gateway Help Desk Privacy Act Statement

Authority: 5 U.S. C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: DHS will use this information to confirm your Infrastructure Protection (IP) Gateway user role and respond to your questions.

Routine Use: This information may be disclosed as generally permitted under 5 U.S.C. §552a(b) of the Privacy Act of 1974, as amended. This includes using the information, as necessary and authorized by the routine uses published in DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System of Records November 25, 2008, 73 Fed. Reg. 71659.

Disclosure: Furnishing this information is voluntary; however failure to provide any of the information requested may prevent the IP Gateway Help Desk from providing assistance or answering your questions.

ATTACHMENT 3

IP Gateway System-Use Disclaimer

The following disclaimer is displayed for and must be accepted by all users prior to accessing the IP Gateway:

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.