The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Senior Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Infrastructure Protection (IP) Gateway**		
Component:	National Protection and Programs Directorate (NPPD)	**Office or Program:**	Office of Infrastructure Protection
TAFISMA Name:	**IP Gateway**	**TAFISMA Number:**	**PRE-03667-GSS-03667**
Type of Project or Program:	IT System	**Project or program status:**	Operational

PROJECT OR PROGRAM MANAGER

Name:	**Jennifer Steinhagen**		
Office:	**Infrastructure Information Collection Division**	**Title:**	Program Manager
Phone:	**703-235-9520**	**Email:**	Jennifer.steinhagen@hq.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	**Michael Skwarek**		
Phone:	**630-252-0572**	**Email:**	mskwarek@anl.gov

ROUTING INFORMATION

Date submitted to Component Privacy Office:	January 14, 2014
Date submitted to DHS Privacy Office:	January 23, 2014
Date approved by DHS Privacy Office:	February 19, 2014

SPECIFIC PTA QUESTIONS

1. Please describe the purpose of the project or program:
Please provide a general description of the project and its purpose in a way a non-technical person could understand.

The primary purpose of the IP Gateway is to provide a framework for enhanced sharing of infrastructure information. The IP Gateway is a web-based portal that supports the collection, analysis, and dissemination of infrastructure information. Through its capabilities it supports numerous National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) activities and tasks including data collection and management, operational scheduling, report management, and analysis for comprehensive risk assessment, management/ mitigation, and contingency planning.

Various PTAs were completed for applications within the IP Gateway, formerly the Linking Encrypted Network System (LENS), between 2010 and 2011. A Privacy Impact Assessment was published for LENS on February 9, 2012. NPPD is conducting this PTA to update and consolidate all of the PTAs for applications that reside on the IP Gateway into a single PTA which covers all of their capabilities.
The applications that reside on the IP Gateway can be grouped into three main capabilities:

- Data Collection and Web Based Dashboards
- Information Sharing and Training Tools
- Administrative, Management and Reporting Capabilities

Capability Group 1: Data Collection and Web Based Dashboards
The purpose of the data collection and web based dashboards is to collect and display data for the Protective Security Advisors (PSAs), Sector Specific Agencies (SSAs) and the State, Local, Tribal, and Territorial (SLTT) communities. These capabilities allow for analysis of performance and review of vulnerabilities of Critical Infrastructure (CI). The focus is on physical security, cybersecurity, security force, security management, information sharing, protective measures, and internal and external dependencies. The web based dashboards are used to convey, track, manage and graphically display information collected by the PSAs or through incident/suspicious activity reporting. Geospatial information is collected through data collection functions and updated to DHS geospatially enabled data. This data is then used to display the reports and maps of CI facilities in a query.

Capability Group 2: Information Sharing and Training Tools
The information sharing and training functionality include dynamic sharing of data and information sources across the critical infrastructure community, including facility owners and operators and SLTT community partners. The information sharing tools enable 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 managed within the individual applications based on a user's need-to-know. The movement of information and data through the communication channels across the organization (from the field personnel to HQ), along with the short and long term storage capabilities, allows the archival, retrieval, and manipulation of data at will. The ability to provide simple knowledge management provides relevant material for designing training content for both employees as well as stakeholders.

Capability Group 3: Administrative, Management and Reporting Capabilities

The administrative, management and reporting functionality is used to schedule, track, coordinate, and maintain activities in the field. This set of capabilities allows both field personnel and IP leadership 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 the critical functions to protect our Critical Infrastructure.

Other changes to the IP Gateway include:
A new User Interface to make functionality and operation more "user friendly" as well as appear in a more fluid and updated manner. This will allow the addition of users from the State and local levels onto the IP Gateway to enable a better interconnection between DHS and its SLTT stakeholders. The IP Gateway is also undergoing an expansion to allow more concurrent users as well as total users.

Individual PTAs will no longer be completed for each application on the IP Gateway, instead the NPPD Office of Privacy will work with the IP Gateway program to review and assess new applications, as well as changes to existing applications to ensure there is proper privacy compliance documentation in place and that all privacy risks are being managed appropriately.

2. Project or Program status		Update	
Date first developed:	**October 1, 2009**	**Pilot launch date:**	**N/A**
Date last updated:	**February 9, 2012**	**Pilot end date:**	**N/A**

3. From whom does the Project or Program collect, maintain, use or disseminate information? *Please check all that apply.*	☒ DHS Employees ☒ Contractors working on behalf of DHS ☒ Members of the public ☐ This program does not collect any personally identifiable information[1]

4. What specific information about individuals could be collected, generated or retained?
Please provide a specific description of information that might be collected, generated or retained such as names, addresses, emails, etc.

The IP Gateway collects the following PII for user registration:

1. Full name

[1] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

2. Citizenship (US Yes/No)
3. Organization
4. Type of employee (State, Local, tribal, Contractor)
5. Role of Duties in Government
6. Work Address
7. City
8. State/ Territory
9. Zip code
10. Work email address
11. Office phone number
12. Work cell phone number
13. Whether the person is Protected Critical Infrastructure Information (PCII) trained
14. Name of federal employee from the Office of Infrastructure Protection sponsoring access
15. Whether the individual's organization provides annual Cybersecurity and Awareness Training (Yes/No)
16. Role or reason access is required

Applications that reside on the IP Gateway may contain business contact information for users and other critical infrastructure partners. This contact information would consist of full name, email address, work address and phone numbers (office and cell) for the designated point-of-contacts (POCs).

Does the Project or Program use Social Security Numbers (SSNs)?	No
If yes, please provide the legal authority for the collection of SSNs:	Click here to enter text.
If yes, please describe the uses of the SSNs within the Project or Program:	Click here to enter text.

5. Does this system employ any of the following technologies: *If project or program utilizes any of these technologies, please contact Component Privacy Officer for specialized PTA.*	☐ Closed Circuit Television (CCTV) ☐ Sharepoint-as-a-Service ☐ Social Media

	☐ Mobile Application (or GPS) ☐ Web portal[2] ☒ None of the above
If this project is a technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
N/A	

6. Does this project or program connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
7. Does this project or program connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place. N/A

[2] Informational and collaboration-based portals in operation at DHS and its components which collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or who seek to gain access to the portal "potential members."

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.

Appendix: IP Gateway Inventory (see attached spreadsheet)

The NPPD Office of Privacy will not update this PTA every time an application is added to or removed from this inventory. NPPD will maintain the inventory internally and can share it with DHS Privacy whenever needed. The NPPD Office of Privacy will meet with the IP Gateway Program POCs quarterly to review the inventory and determine if any applications need to be added or removed. The NPPD Office of Privacy will also use the newly developed NPPD IP Gateway Privacy Checklist (attached) to review and assess all new applications and determine whether the application is covered under this PTA or if an update is required.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Emily Andrew**
Date submitted to DHS Privacy Office:	January 23, 2014

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed.

The NPPD Office of Privacy recommends that this is a Privacy Sensitive System and that an update to the DHS/NPPD/PIA-022 – Linking Encrypted Network System (LENS) Linking Encrypted Network System (LENS), February 9, 2012 is required. Given a number of the changes, updates, migrations and dispositions are currently ongoing and are not scheduled to wrap-up until Summer 2014 (see IP Gateway Inventory and IP Gateway Applications Disposition PTA for more information), the NPPD Office of Privacy recommends that the PIA update be completed by February 2015 to accommodate these changes and correspond with the 3-year mandatory review cycle for the current PIA. The PII collected for user access is covered under DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Lindsay Lennon**
Date approved by DHS Privacy Office:	February 19, 2014
PCTS Workflow Number:	**1006201**

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.

Determination:

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☐ Privacy Act Statement required.

☒ Privacy Impact Assessment (PIA) required.

☒ System of Records Notice (SORN) required.

PIA:	PIA update is required. If covered by existing PIA, please list: Click here to enter text.
SORN:	System covered by existing SORN If covered by existing SORN, please list: DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 Fed. Reg. 70,792

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

PRIV agrees that the IP Gateway is a privacy sensitive system requiring PIA and SORN coverage. PRIV agrees that DHS/NPPD/PIA-022 requires an update. PRIV agrees that this update will take place by February 2015 since the system will be undergoing changes until Summer 2014. The DHS/ALL-004 GITAARS SORN provides SORN coverage. PRIV agrees with NPPD's request to manage the addition of new systems through quarterly meetings with program POCs, a checklist, and internal tracking spreadsheet when these systems do not require a PTA update. When, based on the checklist or other circumstances, a new or updated system require an update to this PTA, NPPD will submit an updated or new PTA to PRIV for review.