Privacy Impact Assessment
for the

Linking Encrypted Network System (LENS)

DHS/NPPD/PIA-022

February 09, 2012

Contact Point
Timothy Huddleston
Infrastructure Information Collection Division
Office of Infrastructure Protection
National Protection and Programs Directorate
(703) 235-3010

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Critical Infrastructure Technology and Architecture (CITA) Project maintains the Linking Encrypted Network System (LENS), a data repository and application set that acts as a network of online portals or modules, allowing authorized users to obtain, post and exchange information and access common resources. NPPD conducted this PIA to examine the privacy impact associated with the collection of personally identifiable information (PII) related to individuals who are LENS users or seeking access to LENS, as well as PII related to points of contact (POCs) that may be maintained within the LENS data repository. NPPD will conduct separate PIAs, as necessary, for those modules or applications residing on the LENS platform where the scope of the collection is beyond that of this PIA.

Overview

Background

The CITA Project provides a strategic and coordinated approach for enterprise data management and information technology development that enables the secure sharing of infrastructure information to enhance the understanding of our Nation's critical infrastructure. The overarching role of the CITA Project is to provide a framework and governance structure that ensures that its underlying systems, applications, and tools conform to DHS and enterprise architecture standards, including privacy. LENS is one of several systems covered by the CITA Project and is currently being leveraged by NPPD's Office of Infrastructure Protection with the potential to expand to other components of NPPD.

LENS is an informational/collaboration-based portal that is primarily being used in support of NPPD's collection and maintenance of data vital to the effective identification, categorization, and protection of the Nation's critical infrastructure, in accordance with Homeland Security Presidential Directive – 7. LENS provides a means of communication that allows individuals from many different geographic areas to share infrastructure information and to collaborate in a meaningful way. As a portal, LENS consists of a web-based interface, user registration and authentication, log-in and verification, and a number of modules, which can be defined as independent software applications that provide users with specific functionalities. These modules support specific functions within NPPD such as: the collection, analysis, and review of infrastructure information; the dissemination of relevant, infrastructure information to authorized users and facilitates; and the collaboration with NPPD's partners. Below are some examples of LENS modules and how they support these functions:

- The Infrastructure Survey Tool supports the collection of infrastructure information, allowing Protective Security Advisors to conduct security surveys through both direct entry and supporting on-site assistance visits.
- The PMI Dashboard provides a visual dashboard that shows the overall protective measure index for all 18 critical infrastructure and key resources (CIKR) sectors in comparison to each other.
- The Infrastructure Information Collection System provides users with the ability to easily access, search, retrieve, visualize, analyze, and export infrastructure data from the LENS data repository, as well as external data sources, through a single interface.
- The LENS data repository stores all data collected from the modules on the LENS platform. Data contained within the LENS data repository is logically partitioned, and user access controls are implemented so that only those individuals with a need to access the information are granted access to it.

The primary purpose of LENS is to provide a framework for enhanced sharing of infrastructure information. NPPD utilizes a number of resources to collect infrastructure information. For example, an analyst may use the Internet to research information required to identify a facility, such as the address or latitude and longitude coordinates, conduct a site visit to obtain information from a facility owner/operator, or retrieve information from other NPPD systems that maintain infrastructure information. As LENS data is related primarily to infrastructure, the content of information exchanged through the portal does not contain PII, except for limited contact information associated with its users or with infrastructure assets. Specifically, NPPD collects PII from individuals in two categories:

1) LENS users (e.g., DHS employees or contractors who are verified during the registration process to ensure they are authorized to use LENS); and

2) Points of contact (POCs), such as private sector partners or stakeholders associated with specific infrastructure assets.

<u>PII Collected from LENS Users</u>

A potential LENS user requests access to LENS by completing a LENS Account Request Form, which collects the following information:

a. Full name;

b. Citizenship;

c. Organization;

d. Directorate/Division/Branch;

e. Street address;

f. City;

g. State/Territory;

h. ZIP code;

i. Email address;

j. Office phone number;

k. Cell phone number;

l. Federal employee or contractor;

m. Protected Critical Infrastructure Information (PCII) trained;

n. Name of federal employee from Office of Infrastructure Protection sponsoring access to LENS; and

o. Role or reason access is required.

Certain modules on the LENS platform may require users to submit application-specific request forms or require DHS representatives to nominate individuals for access to a DHS system. In such cases, NPPD may collect the same (or fewer) data elements collected through the LENS Account Request form. Additionally, NPPD may collect the name and business contact information of the DHS representative sponsoring the applicant.

The LENS System Administrator is responsible for reviewing/approving the LENS Account Request form and creating the LENS user account. LENS users are granted access to modules on the LENS platform through role-based access, lightweight directory access protocol (LDAP) groups, memberships, and Oracle Label based security. Users are only given access to the LENS modules that they have been approved for.

Steps taken to protect privacy include the requirement that all LENS users are vetted by their respective NPPD mission area. Additionally, all LENS users are required to sign the system's rules of behavior, which dictate how the system and data from the system may be used. Finally, the data are protected from access in transit by FIPS-140-2 hardware encryption.

<u>PII Collected from POCs</u>

NPPD generally collects PII related to POCs that are associated with a particular infrastructure or asset. POCs could include, but are not limited to, private sector partners or stakeholders associated with specific infrastructure assets. In such cases, PII is stored as part of the profile of the facility or asset and is maintained in the LENS data repository. The PII that NPPD collects from POCs is limited to the following:

a. Full name;

b. Email address;

c. Office phone;

d. Cell phone number; and

e. Business address.

NPPD uses 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 and operators to convey information to help protect their infrastructure.

<u>Scope of this PIA</u>

A full list of modules housed on the LENS platform is listed at Appendix A. As NPPD expands LENS beyond the collection of infrastructure information, additional modules may be added to the LENS platform. This PIA is intended to cover the current collection of LENS user data and POC information for all modules on the LENS platform, as well as future uses of LENS, which could include collection of non-sensitive PII associated with business contacts, employees, and contractors for collaboration purposes. However, where the scope of the collection of PII for any module is beyond that of this PIA or includes sensitive PII, a separate PIA will be conducted.

While LENS users are limited to DHS employees and contractors, there are infrastructure facility self assessment applications on the LENS platform in which a limited number of sectors, such as the Commercial Facilities and Chemical sectors, may voluntarily submit their facility’s information directly to their respective LENS module. The Risk Self Assessment Tool is an example of an application where a facility may choose to voluntarily submit information about the facility to the self assessment tool directly. However, that facility would not access the tool through the LENS portal and would not have the ability to access other tools on the LENS platform.

Additionally, NPPD may share infrastructure information with its federal, state, or local partners. Such sharing typically occurs in response to a request for information about a particular infrastructure asset. Some data within LENS is considered PCII and may only be shared with PCII Authorized Users who have a need to know. However, as non-DHS entities do not have direct access to the LENS portal, that information is not shared through LENS. Nor does NPPD share PII that is maintained within LENS.

Finally, NPPD ensures the accuracy of infrastructure-related data maintained within the LENS environment through a quality assurance process that involves weekly checks of data to identify gaps and resolve discrepancies between new records and existing records in the LENS data repository. In most cases, NPPD collects PII maintained in LENS directly from the individual, which helps to ensure that PII is accurately maintained.

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?

LENS is primarily used to collect infrastructure information (CII) as authorized by Section 201(d) of the Homeland Security Act [6 U.S.C. §121(d)]. NPPD's Protected Critical Infrastructure Information (PCII) program, authorized by the "Critical Infrastructure Information Act" (6 U.S.C. 131 *et seq.*), controls the protection of the majority of the CII collected in LENS.

1.2 What Privacy Act System of Records Notice(s) (SORN(s))

NPPD collects PII from individuals for the purpose of granting access to the LENS portal. This collection is covered by the Department of Homeland Security system of records titled, "Department of Homeland Security/ALL-004 General Information Technology Access Account Records," published September 29, 2009.

NPPD also collects limited contact information on POCs through modules or applications that are housed on the LENS platform. However, this information is not filed or retrieved by the individual's PII. POC information is generally filed and retrieved by the name of a facility or other asset that the individual is associated with.

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

A system security plan was completed for LENS, and LENS was granted a 3-year Authority to Operate (ATO) on September 8, 2011.

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

NPPD is working with its Records Officer to develop a disposition schedule, which will be sent to NARA for approval.

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.

LENS is a part of the NPPD - CITA investment with the UPI of: 024-65-01-06-01-9502-00.

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.

Through LENS, NPPD maintains PII for two categories of individuals: (1) LENS users (e.g., DHS employees or contractors who are verified during the registration process to ensure they are authorized to use LENS); and (2) POCs, such as private sector partners or stakeholders associated with specific infrastructure assets.

PII collected from LENS users

DHS employees and contractors seeking access to LENS must complete a LENS Account Request Form and submit the following information:

a. Full name;

b. Citizenship;

c. Organization;

d. Directorate/Division/Branch;

e. Street Address;

f. City;

g. State/Territory;

h. ZIP code;

i. Email Address;

j. Office Phone Number;

k. Cell Phone Number;

l. Federal employee or contractor;

m. PCII Trained;

n. Name of federal Employee from IP sponsoring access to LENS; and

o. Role or Reason Access is Required.

Certain modules on the LENS platform may require users to submit application-specific request forms or require DHS representatives to nominate individuals for access to a DHS system. In such cases, NPPD may collect the same (or fewer) data elements collected through the LENS Account Request form. Additionally, NPPD may collect the name and business contact information of the DHS representative sponsoring the applicant.

Once a registered member of the LENS portal, a LENS user may voluntarily post information such as comments, documents, links, or calendar entries. The content of information posted to shared spaces does not contain PII other than associating the post with the limited LENS user contact information.

PII Collected from POCs

NPPD collects information on critical infrastructure as part of its mission, which includes identifying POCs for those facilities and assets associated with critical infrastructure. NPPD collects business contact information for POCs, which is accessible through the LENS data repository, but filed/retrieved by the name of the facility or asset, and includes the following:

a. Full name;

b. Email address;

c. Office phone;

d. Cell phone number; and

e. Business address.

While contact information for POCs is currently associated with infrastructure assets, future uses may include collecting limited PII to facilitate the exchange of contact information for distribution lists or to facilitate working relationships between partners. The contact information would be limited to non-sensitive PII, collected directly from our partners, and would only be used for the purpose for which it was collected.

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

One of the primary functions of LENS is to provide a “one-stop shopping” experience for infrastructure information, which can then be used for event and incident planning, mitigation, and response activities. To accomplish this, LENS collects data from multiple sources. Examples of sources for infrastructure information include:

- Open source information – NPPD may use open sources (e.g., Internet) to collect information to identify a particular facility or asset. For example, NPPD may use Internet sources to retrieve the address of a facility or its latitude or longitude coordinates.

- Other IT systems or existing datasets – LENS obtains infrastructure information from the Automated Critical Asset Management System (ACAMS), Environmental Protection Agency Off-site Consequence Analysis (EPA-OCA) Risk Management Program data, and Homeland Security Infrastructure Program (HSIP).

- Directly from infrastructure owners/operators – NPPD collects information directly from individuals associated with a particular infrastructure or asset. For example, NPPD may collect infrastructure information during a site visit or through its working relationship with a facility.

While NPPD utilizes a number of resources to collect infrastructure information, PII is always collected directly from the individual.

For example, all potential LENS users submit their registration information directly to NPPD. A LENS user submits PII to NPPD using the general LENS Account Request Form or one of the application-specific user request forms. Currently, NPPD accepts both online registration forms and hard copy submissions. Future action is planned to consolidate all LENS registration processes into a single, online registration process.

Information related to POCs for infrastructure facilities and assets comes directly from infrastructure asset owners and operators through working with them in supporting the NPPD mission. For example, NPPD may collect POC information from a facility while conducting a site visit. Such information would be added to the profile for the facility and is not filed or retrieved by the POC's name or other 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.

NPPD does not use commercial sources or publicly available data to collect information for LENS registration or access purposes; nor does NPPD utilize such sources to collect PII related to POCs.

The LENS data repository may include information collected from publicly available data for the purpose of completing and verifying basic identifying information in submitted site records and for developing background reports on infrastructure that will be later visited by DHS. This collection does not include PII.

WebEOC[1] is an example of a LENS module that collects information from the Internet and news media to support the National Infrastructure Coordinating Center's (NICC's) mission to manage information related to CIKRs. This collection is covered by NPPD's Privacy Impact Assessment, DHS/NPPD-017(a) NICC SARS: National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative Update, published August 12, 2011, and the DHS/NPPD-001 – NICC Records System, 75 FR 69693, published November 15, 2010.

2.4 Discuss how accuracy of the data is ensured.

NPPD ensures data accuracy by collecting information directly from individuals seeking access to LENS and from infrastructure POCs. Additionally, NPPD utilizes a quality assurance (QA) process by which records are verified and document holdings are updated. When a new asset record is created, the data QA team checks the infrastructure information submitted by the user for duplication against the existing infrastructure records in the LENS data repository. Specifically, the LENS data QA team verifies the facility name, location, and infrastructure information and completes any missing information necessary to identify the facility (to the extent possible) based on public information sources. Each week LENS performs an automated check for infrastructure record changes by any person other than a member of the LENS data QA team. The LENS data QA team then reviews and approves or rejects the changes. Each year the team conducts multiple reviews of various aspects of the entire repository to check for data gaps or coding inconsistencies to resolve the issues to the extent possible. The LENS data QA team does not verify submitted records that are not verifiable, not completed, or corrected by the LENS user. These records are moved to a deprecated record table by the LENS QA team.

For document holdings, LENS performs a weekly automated check to identify new documents. The LENS QA team opens and checks all newly loaded documents to ensure the documents were attached to the appropriate record(s), the document labeling is appropriate, and security protections are in place. Where appropriate, the LENS QA team establishes a revision cycle, to ensure the document remains up to date.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: As LENS collects information from multiple sources, there is a risk that more information than is necessary may be collected or that information collected may be inaccurate.

[1] See Appendix A.

<u>Mitigation:</u> NPPD determined that this risk is minimal, as no PII is used to make any decisions about an individual, and is fully mitigated in that the PII collected for access/registration and for POC information is collected directly from the individual. Additionally, NPPD's QA process ensures the accuracy of data maintained in the LENS data repository, which would include data on infrastructure assets and their associated 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 registration information from DHS employees and contractors to facilitate requests for access to the LENS portal and to validate those individuals as authorized users of specific modules on the LENS platform. Information collected for this purpose is consistent with the requirements of the DHS Sensitive Systems Handbook 4300A. Upon registration, the use of that PII facilitates the information and collaboration purposes of the portal and is consistent with the routine uses in the System of Records Notice for "Department of Homeland Security/ALL-004 General Information Technology Access Account Records," published September 29, 2009.

NPPD uses POC information stored in the LENS data repository in order to facilitate communications with stakeholders, generally related to critical infrastructure and key resources.

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 such results.

No, LENS is not used to discover or locate a predictive pattern or anomalies. LENS does not analyze or manipulate PII.

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

Currently, LENS users are primarily federal employees and contractors of IP. The following other DHS components have access to LENS, however, their roles are limited to entering data into the Infrastructure Data Call Application:[2] NPPD's Office of Cyber Security

[2] See Appendix A.

and Communications and Federal Protective Service, the Transportation Security Administration, the United States Coast Guard, and U.S. Immigration and Customs Enforcement.

As NPPD continues to add modules to LENS, it is anticipated that other components of NPPD will also have roles within LENS; however, access will always be limited to those modules for which an employee or contractor has a business need.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse of PII, such as sharing of information with individuals without a need-to-know.

Mitigation: LENS users have access to the respective LENS module(s) (which may contain POC information) that support their role within their organization. For example, a LENS user that is a NICC watch stander will have access to the NICC WebEOC tool, the tool that supports the specific functions of the NICC. However, that watch stander, unless deemed necessary in fulfilling the watch stander's role, will not have access to the Infrastructure Survey Tool, the tool used by IP Protective Security Advisors to collect infrastructure vulnerability information from asset owners and operators.

LENS user PII information is only accessible to the LENS system 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 or other infrastructure information. The risk is further mitigated in that all LENS users are vetted by their respective NPPD mission area and are required to sign the system's rules of behavior, which dictate how the system and data from the system may be used. LENS users are warned that misuse is punishable by civil or criminal proceedings when they connect to LENS. Finally, the data is protected from access in transit by FIPS-140-2 hardware encryption.

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.

In order to receive access to LENS, individuals must provide the required personal information. Access to LENS is completely voluntary, and individuals may decline to participate by not providing their contact information, although this will result in the individual not gaining access to LENS. Further, LENS users are presented with Privacy Act statements, upon accessing the individual modules, which provide notice as to how their information will be used. A sample Privacy Act statement from the Infrastructure Data Call Application is provided at Appendix C.

NPPD collects POC information directly from the individual, and such information is provided to NPPD voluntarily. At any time, the individual may opt not to participate with the data collection.

Finally, NPPD collects information during the course of facility assessments. Participation with these assessments is completely voluntary, and NPPD provides the facility owner/operator with a brief notice that describes the purpose of the assessment and what information will be requested.

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

As stated in the response to question 4.1, most information collected through LENS is done so on a voluntary basis and, as such, individuals can elect not to participate. The use of an individual's information is for contact purposes only. Personal information is not used in any other way. All individuals may request removal of their information by contacting the LENS Help Desk, who will coordinate the request with the module program manager. The Program Manager will work in coordination with the NPPD Office of Privacy to ensure the removal of the requested information in accordance with DHS standards.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that an individual may not understand how PII is being used.

Mitigation: PII in LENS is limited primarily to business contact information. Individuals voluntarily register to become members of the LENS portal to collaborate and exchange information with other members; thus individuals are well aware of the purpose for the collection. Because the PII collected from LENS users consists almost entirely of business contact information and is only accessible by the system administrators, NPPD determined that the privacy risk for LENS users is minimal. This risk is fully mitigated in that NPPD provides notice in the form of Privacy Act statements upon entering specific LENS modules, and in the System of Records Notice for "Department of Homeland Security/ALL-004 General Information Technology Access Account Records," published September 29, 2009.

With regard to PII collected from infrastructure POCs, the risk is also minimal, as the information is provided to NPPD voluntarily and is limited to business contact information that would normally be provided in the course of conducting business. This risk is mitigated in that, when conducting facility assessments, NPPD provides the POC with a brief notice that describes the purpose of the assessment and what information will be requested.

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.

NPPD maintains the PII collected for the purposes of establishing a LENS user account indefinitely. Per National Institute of Standards in Technology (NIST) Special Publication 800-53 control AC-2, LENS user accounts that are no longer in use are disabled, but not deleted. However, inactive records not required by DHS/NIST security will be deleted from LENS after six years, in accordance with the SORN.

Most infrastructure information collected via LENS is retained, considered permanent, and cannot be deleted. The proposed records retention schedule is based on the fact that infrastructure assets, such as large buildings, can remain in place for tens or hundreds of years. PCII data can be deleted upon the request of the submitter of that information.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The risk associated with maintaining PII longer than relevant or necessary is unauthorized disclosure of PII.

Mitigation: This risk is mitigated in that certain categories of information, such as PII associated with POCs or PCII, can be removed from LENS at the request of the individual or submitter. As for the PII collected from LENS users, NPPD mitigates this risk by ensuring that all PII retained is securely stored and protected in accordance with the LENS System Security Plan. DHS Security has reviewed and certified the combination of physical and cyber security measures in place at the federally owned facility that hosts LENS. LENS has also been reviewed by the DHS Inspector General's office and found to be securely configured and managed.

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.

Currently, DHS is the only agency that accesses LENS for the NPPD-collected data in LENS’s data repository. DHS may share infrastructure information with non-DHS entities. However, this is typically done in response to a request for information (RFI) from another federal, state, or local entity. At this time, non-DHS entities do not have access to such information through the LENS portal.

Within LENS, there are infrastructure facility self assessment applications in which a limited number of sectors, such as the commercial facilities and chemical sectors, may voluntarily submit their facility’s information directly to their respective LENS module (e.g., Risk Self Assessment Tool, Voluntary Chemical Assessment Tool[3]). This information is not shared with other private sector entities outside of the sector voluntarily submitting the information or reused for purposes outside of the intended use of the originating application. The information collected by the tools for the sectors is voluntarily submitted, and not validated or verified by NPPD. That is, it does not fall within the LENS data QA team process.

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

LENS falls under the DHS/ALL-004 - Department of Homeland Security General Information Technology Access Accounts Records System (GITAARS), 74 FR 49882 (September 29, 2009). As documented in the GITAARS SORN, “all persons who are authorized access DHS information technology resources, including employees, contractors, grantees, private enterprises and any lawfully designated representative of the above and including representatives of federal, state, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the DHS mission. Also covered by this system are

[3] See Appendix A.

individuals who serve on DHS boards and committees; individuals who have business with DHS and who have provided personal information in order to facilitate access to DHS information technology resources; and individuals who are points of contact provided for government business, operations, or programs, and the individual(s) they list as emergency contacts."

POC information is not filed or retrieved by the individual's PII, but rather is filed/retrieved by the name of a particular facility or other asset that the individual is associated with. This information is not covered by the Privacy Act and is not shared outside of DHS.

6.3 Does the project place limitations on re-dissemination?

LENS user PII cannot be re-disseminated outside of DHS, as the information is collected for the sole purpose of granting access to LENS and its modules. As for the PII associated with POCs, some PII is intertwined with data contained within the LENS data repository that is PCII. 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 LENS 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.

LENS 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 LENS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that PII collected for specific access purposes to the LENS data repository will be shared outside DHS.

Mitigation: Any potential risk related to information sharing is mitigated, in that DHS may share infrastructure information, such as facility assessments or other information characterizing sector risks outside of DHS; however, PII is not shared along with that information.

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?

LENS users do not have direct access to their information through LENS. However, they can access or correct their information at any time by contacting the LENS Support Help Desk.

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

All individuals may request access to information about them by submitting a Freedom of Information Act/Privacy Act (FOIA/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/PA request at http://www.dhs.gov/xfoia/editorial_0316.shtm.

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

LENS users may update their contact information by contacting the LENS Support Help Desk. POCs may update erroneous information by making a request to the NPPD component that collected the information from them.

All individuals 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?

While conducting a site assessment, NPPD will inform the infrastructure owner/operator or other POC that he or she may update their information by contacting the provided point of contact.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may be unaware of their redress options.

Mitigation: This risk is mitigated in that most PII maintained within LENS pertains to LENS users, in which case those users have the ability to access and correct their data via the LENS Support 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. All individuals are provided notice of their redress options in this PIA.

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?

LENS uses a number of continuous monitoring tools to maintain a secure baseline and to prevent unauthorized access. These tools include centralized logging using Splunk and a vulnerability scanning tool called Scavenger. In addition to self-audits, LENS has been subject to multiple audits by the Government Accountability Office and the DHS Office of Inspector General.

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

Some data contained within LENS is PCII, as defined by the CII Act § 212(A). Access to PCII requires PCII training and designation as a PCII Authorized User. Other information within LENS does not require specialized training; however, all DHS employees and contractors are required to participate in privacy training annually.

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

LENS consists of a number of modules. Users are granted access to the modules through role-based access LDAP groups, memberships, and Oracle Label based security. Users are only given access to the LENS modules for which they have been approved. All LENS traffic is encrypted through the use of Common Criteria Certified Juniper Secure SSL appliances, using TLS1.0.

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 respective application owner in coordination with the IP Data Governance Board and IP Privacy Point of Contact. Agreements, access, MOUs, and uses of information are coordinated with and sent to the NPPD Senior Privacy Officer and counsel, as appropriate.

Responsible Officials

Timothy Huddleston
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

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Systems (modules) covered by the LENS PIA:

1) **Critical Manufacturing Assessment Tool (CMAT)** – A comprehensive risk assessment tool to improve and/or standardize the way DHS's private sector partners collect and manage information for the security planning process, from initial collection of data to risk assessment to countermeasure implementation. Private sector partners may voluntarily submit their business contact information to DHS.

2) **Dams Sector Analysis Tool (DSAT)** – An analysis tool that will collect infrastructure information from Dam Facility owners and operators. Private sector partners may voluntarily submit their business contact information to DHS.

3) **Emergency Services Self Assessment Tool (ESSAT) –** An application designed for stakeholders within the Emergency Services, Critical Infrastructure and Key Resources sector, allowing voluntary identification of vulnerabilities and risks pertaining to particular facilities. Private sector partners may voluntarily submit their business contact information to DHS.

4) **Infrastructure Data Call Application (IDCA)** – Sector Specific Agencies (SSA) and State and Territorial Homeland Security Advisors (HSAs) will use this Application to prepare and submit their recommendations for the DHS Level 1 /Level 2 list of CIKR assets. The IDCA User Management Application stores limited information about IDCA users such as name, address, phone number, and organization.

5) **Infrastructure Information Collection System (IICS)** – An information system providing users with the ability to easily access, search, retrieve, visualize, analyze, and export infrastructure data from multiple sources through a single interface. As a search engine, IICS does not collect data, but allows users access to several data sets, which could include PII such as business contact information associated with POCs for infrastructure assets.

6) **NIPP Metrics Portal –** The NIPP Metrics Portal is a living tool that will evolve in response to the needs of the National Infrastructure Protection Plan (NIPP) user community in meeting the requirement that SSAs provide updated programmatic metrics information to the Department of Homeland Security twice annually. The Portal will also be used to collect information for Core, Partnership, Sector-Specific, and other metrics that may be developed. Business contact information is collected for the sole purpose of granting access to the portal.

7) **PSCD LENS –** A set of applications or tools utilized by the Office of Infrastructure Protection, Protective Security Coordination Division (PSCD). The tools collect limited PII associated with users and with infrastructure assets. A complete list of tools is listed in Appendix B.

8) **Risk Self Assessment Tool (RSAT)** – The RSAT application guides the self-assessment of incident consequence and countermeasures to repel the incident. After completion, the assessor receives a summary report and the assessment is submitted to DHS for review. RSAT does not collect PII beyond information associated with its users.

9) **Taxonomy Comments** – A tool that used to collect comments to the IP Taxonomy. This tool does not collect PII beyond information associated with LENS users.

10) **Voluntary Chemical Assessment Tool (VCAT)** – A voluntary assessment for the chemical Critical Infrastructure and Key Resources sector used to assess vulnerabilities and risks pertaining to a particular facility. Private partners may voluntarily submit their business contact information to DHS.

11) **WebEOC** – A multi-purpose web-based application designed to assist and support NICC watch standers in managing information requests, incident reporting, and suspicious activity reporting in order to facilitate coordination and information sharing with the CIKR sectors. The NICC produces consolidated CIKR reports for incorporation into the Federal Interagency DHS Common Operating. WebEOC is also covered under NPPD's Privacy Impact Assessment, DHS/NPPD-017(a) NICC SARS: National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative Update, published August 12, 2011, and the DHS/NPPD-001 – NICC Records System, 75 FR 69693, published November 15, 2010.

Appendix B

PSCD LENS refers to a set of applications or tools utilized by the Office of Infrastructure Protection, Protective Security Coordination Division.

PSCD LENS tools include:

Data Collection Tools

1) **Infrastructure Survey Tool (IST)** – A security survey of critical infrastructure facilities conducted by the Protective Security Advisors (PSA). Majority of the information collected is PCII.
2) **Infrastructure Survey Tool DEV** – This is the development application for the Infrastructure Survey Tool listed above.
3) **Site Assistance Visit Builder** – This is the tool used to collect the information supporting the Site Assistance Visit, a vulnerability assessment tool used by the Vulnerability Assessments Branch (VAB). Majority of the information collected is PCII.

Information Display Tools

4) **PSA Operations** - An application that maintains key contacts for each PSA to support continuity of operations activities. It also incorporates Domestic Incident Tracking and a Specials Events tracking functionality.
5) **PMI Dashboard v3** – The tool is a tool in development and provides a visual dashboard that shows the overall protective measure index for all 18 sectors in comparison to each other. The information supporting this visual dashboard comes from the IST. Majority of the information collected is PCII.
6) **PMI Dashboard State** – The tool is a tool in development and provides a visual dashboard that shows the overall protective measure index for all 18 sectors in comparison to each other at the State level. Majority of the information collected is PCII.

Administrative, Management, and Reporting Tools

7) **Protective Security Advisor (PSA Tracker)** – A scheduling, reporting, and visit support application for PSAs with functionality similar to SAV Tracker.
8) **PSA Tracker DEV** – A developmental tool in implementing updates and changes to PSA Tracker.

9) **Weekly Activity Report (WAR)** – Integrated with Tracker, this application enables staff that support SAVs and other activities to consolidate their schedules into one view.

10) **Background Package Builder (BP Builder)** – A web based document creation tool that guides analysts through the process of building background reports on infrastructure elements.

Information Sharing and Training Tools

11) **Infrastructure Protection Report Series (IPRS)** – A web application to request access to Characteristics and Common Vulnerabilities, Potential Indicators, and Protective Measures (CV/PI/PM) papers and an independent site that allows access to CV/PI/PM papers.

12) **Reference Document Editor –** A tool used to add, edit and change the availability of training modules listed in the Reference Documents section.

13) **Reference Documents** – A tool used for storing available training modules for SAV, BZP, PCII and other general training documents.

14) **System Training** – A tool used for storing key reference and background materials to help potential field team members. The materials are organized within Training Modules. All completed modules will be tracked within the tool. Currently contains the same modules as the Reference Documents portal.

15) **Infrastructure Survey Tool Test –** This tool is used by a test population to test the code developed in the Infrastructure Survey Tool DEV for any glitches or suggestions before being finalized.

16) **National Infrastructure Simulation Analysis Center (NISAC) Reports** – A tool used for storing all available NISAC Reports.

17) **Risk Management Division (RMD) Documents –** This is a portal which contains historical one-pagers and documents for RMD and was last updated around 2006.

18) **SAV Latest –** This is a portal with upload/download capabilities for the storage of information for SAV teams. Each SAV team has a folder in this portal which allows for the sharing of documents back and forth between the National Guard and Argonne National Lab.

19) **Upload\Download –** A tool used to store uploaded documents for sharing amongst other LENS users in the field. It enables the sharing of large documents, briefings, data, and graphics.

20) **Enhanced Critical Infrastructure Protection (ECIP) LENS Executive Summary** This contains the Executive Summaries for completed ECIPs as well as dashboard comparisons and instructions for the IST Builder.

21) **Outage and Service Restoration Papers** – A tool used to store documents outlining critical needs for the restoration of Critical Infrastructure in the case of a significant service interruption.

22) **Entergy Project –** A portal used to store the compilation of all products created during the Entergy Project. The information stored includes the final report and all surveys conducted in support of the Entergy Project.

23) **PSCD Computer Based Assessment Tool (CBAT) –** This is a portal that contains folders for each individual project, as well as a best practices folder. This portal also houses the final product for each project. Both VAB and FOB CBAT projects are included in this portal.

Appendix C

Privacy Act Notice

Authority: 49 U.S.C. §114 authorizes the collection of this information.

Purpose: DHS will use this information to provide a framework for enhanced sharing of infrastructure information, which can then be used for event and incident planning, mitigation, and response activities.

Routine Uses: The information will be used by and disclosed to DHS personnel and contractors or other agents who need the information to facilitate requests for access to the LENS portal and to validate those individuals as authorized users of specific modules on the LENS platform. Additionally, DHS may share the information to assist in activities related to identifying the nations critical infrastructure, inform homeland security grants, and other infrastructure protection and incident response activities.

Disclosure: Furnishing this information is voluntary; however failure to furnish the requested information may delay or prevent the completion of requests for access, homeland security grants, and other infrastructure protection and incident response activities.