Privacy Impact Assessment
for the

Loaned Executive Program

DHS/ALL/PIA-045

September 29, 2014

Contact Point
Karinda L. Washington
External Affairs Specialist
Private Sector Office
Department of Homeland Security
(202) 612-1602

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

Abstract

The Department of Homeland Security (DHS) Private Sector Office (PSO) manages the Department-wide Loaned Executive Program (LEP). The LEP is a special unpaid opportunity for executive-level private sector, academia, and cyber security experts to share their expertise with DHS. Through the LEP, DHS seeks innovative solutions to its homeland security challenges. DHS conducted this Privacy Impact Assessment (PIA) because the LEP collects personally identifiable information from members of the public.

Overview

The Department of Homeland Security (DHS) Private Sector Office (PSO) serves as the Secretary's direct point of contact to the private sector; conducts and coordinates private sector outreach across the Department and directs external engagement with Components to support the Secretary's agenda; advises the Secretary on the impacts of the Department's actions, policies, and regulations on the private sector and provides analysis through its economic unit; encourages direct partnership with the private sector through the use of public-private partnerships and other programs like the Loaned Executive Program (LEP), which places private sector representatives in positions within DHS; and represents DHS on a number of interagency bodies.

Established in 2008, the PSO-administered LEP provides an unpaid opportunity for executive-level private sector, academia, and cybersecurity experts to share their expertise with DHS. As determined by their host DHS Components, participants serve as subject matter experts or senior advisors to DHS leadership to evaluate existing policies, procedures, and training. LEP participants may also provide guidance to the Department on the public-private partnership strategies designed to improve private sector engagement with DHS.

Conditions for Participation

- Be a U.S. citizen;
- Serve in a current senior-level operational management or related position, with a track record of building support for and influencing policy decisions as well as deploying sustainable risk, mitigation, and resiliency capabilities;
- Have extensive private sector leadership experience in identifying and screening personnel in functional areas related to risk assessment, mitigation/preparedness, and incident response;

- Undergo and successfully complete a background investigation for determination of suitability for federal employment. Each position description will identify the requisite clearance level; and
- Submit a Confidential Financial Disclosure Report (OGE Form 450).

Initial LEP appointments are made for a period of at least three months and no more than one year. The Loaned Executive may be reappointed for additional periods with the total appointment not to exceed two years. Applicants will complete an orientation, as well as training, to include security and privacy training before their assignment begins.

An LEP appointment may be terminated by DHS at any time DHS determines that the Loaned Executive:

- Provides services that are no longer needed;
- Has a conflict of interest;
- Violates or refuses to sign a nondisclosure agreement; or
- Performs at an unacceptable level as outlined in the Component assignment description.

Components seeking a loaned executive are required to conduct the following steps:

Step One: Identify the need for a loan executive:

- Work with the Component human capital office to complete and sign an assignment description form.
- Submit the assignment description form to the PSO. PSO will circulate the assignment description form to the Office of the Chief Human Capital Officer (OCHCO), Office of the General Counsel-General Law Division (OGC-GLD), Office of the Chief Procurement Officer (OCPO), and the Designated Agency Ethics Official (DAEO), for approval.
- If the assignment description is approved, the Component will proceed to Step Two.
- If the assignment description is rejected, the Component will contact PSO for further assistance.

Step Two: Solicit applicants

- PSO will post the approved assignment description to the LEP web page. The assignment will remain on the LEP web page until the application deadline.

- Resumes are submitted to the proposing Component. If the Component is not satisfied with the resumes received, the application deadline may be extended.

Step Three: Selecting applicant(s). The proposing Component will:

- Review resumes and conduct interviews.
- Forward the names(s) of the selected candidate(s) to the Component human capital office and PSO.

In collaboration with PSO, the Component human capital office will notify the selected and rejected applicant(s).

Step Four: Clearing selected candidate(s). PSO and the proposing Component human capital office will:

- Forward pre-selection notification and clearance forms[1] to the selected applicant(s).
- Convert completed LEP application forms into a clearance package for submission to the DAEO and the OCPO for approval. If the LEP package is rejected, the Component and PSO will work with the applicant(s) and DAEO and OCPO for resolution.
- If approved, the LEP package is forwarded to the OGC-GLD and OCHCO for approval.
- If approved by OGC-GLD and the OCHCO, package will proceed to Step Five. If rejected, PSO will work with applicant(s), OGC-GLD, and OCHCO for resolution. If a resolution cannot be reached the assignment for the applicant(s) cannot be made, and the package will be returned to the Component human capital office.

Step Five: Preparing applicant(s) for entry on duty. The proposing Component human capital office will:

[1] Selected applicants receive a pre-selection notice that explains a final decision will be made after the successful completion of the vetting process. Applicants are asked to complete all applicable LEP forms, which can be found in Appendices at the end of this PIA. Once they clear the vetting process, they receive an additional notice from the human capital office to commence their security clearance.

- Notify the applicant(s) of their successful pre-clearance approval status. Note: "pre-clearance approval status" refers to the period of time that a Loaned Executive is approved to enter on duty to DHS but has not yet completed its security clearance.

- The Component human capital office will initiate the security clearance through their normal personnel security procedures.

- Once cleared, the Component human capital office will coordinate entry-on-duty.

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?

Section 201 of the Homeland Security Act of 2002 and Executive Orders 9397,[2] 12968, 13526,[3] 13549,[4] and 13636,[5] authorize the collection of this information. Individuals cannot be granted access to classified information unless they have been determined eligible for access based on favorable adjudication of an appropriate background investigation. Additionally, the DHS Office of the Chief Security Officer (OSCO) Personnel Security Division has the authority to conduct investigations, as referenced in the privacy impact assessment, DHS/ALL/PIA-038 Integrated Security Management System (ISMS).[6] While the LEP does not conduct investigations, it collects information to facilitate this process.

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

Information collected by the LEP (i.e., citizenship, Social Security number, Date of Birth, Place of Birth, and standard form questionnaires, etc.) is covered under DHS/ALL-021

[2] Executive Order 9397, as amended by Executive Order 13478, gives agencies the authority to collect Social Security numbers whenever the agency finds it advisable to set up a new identification system for individuals.
[3] Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.
[4] Executive Order 13549 establishes a Classified National Security Information Program designed to safeguard and govern access to classified national security information shared by the Federal Government with state, local, tribal, and private sector entities.
[5] Executive Order 13636, Section 4 (e) "In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on temporary basis."
[6] DHS/ALL/PIA-038 - Integrated Security Management System (ISMS), September 23, 2014, *available at* http://www.dhs.gov/privacy-documents-department-wide-programs.

Department of Homeland Security Contractors and Consultants.[7] Information collected by Component personnel security offices to conduct background investigations is covered by DHS/ALL-023 Department of Homeland Security Personnel Security Management[8] and is not stored by the LEP.

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

As this is not an IT system, a system security plan is not applicable to this program.

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

Yes. All records collected and maintained by the Private Sector Office in support of the Loaned Executive Program are covered by the GRS 1 item 17a, and are destroyed upon the separation of the employee; except for:

- Ethics determination regarding the appointment of an unpaid Loaned Executive to DHS (GRS 25 item 3, "destroy 6 years after the waiver or other agreed-upon determination or action has been issued or undertaken or is no longer in effect, whichever is later"); and

- Office of Government Ethics (OGE) Form 450 Confidential Disclosure Report (GRS 25 item 2(b)(2), "destroy when 6 years old; except documents needed in an ongoing investigation will be retained until no longer needed in the investigation").

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.

No, the PRA does not apply. LEP applicants are temporary Loaned Executives and are considered DHS employees for PRA purposes.

---

[7] DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179 (October 23, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-10-23/html/E8-25205.htm.
[8] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

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.

To minimize the collection of personally identifiable information (PII), the LEP process is two-fold, and sensitive PII is only collected from those candidates who are approved for the LEP based on information submitted as part of the first step of the clearance application process.

Step one: The applicant must provide the following:

- Full name;
- Resume;
- Company name;
- Business title;
- Business physical address;
- Business email address;
- Business phone number;
- Business relationship with the sector;
- U.S. Citizen (yes/no); and
- If the individual is deemed suitable for LEP, the Component human capital office contacts the applicant directly to complete the second step, which requires the applicant to provide the remaining sensitive PII needed to begin the security clearance process.

Step two: The applicant must provide the following:

- Date of birth;
- Place of birth; and
- Social Security number (SSN).

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

All information that the LEP collects as part of the application and security clearance process are collected directly from the applicant.

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

While commercial sources may be used by the Office of Personnel Management (OPM) or the Personal Security Division in support of their background investigations (e.g., to perform credit checks), no commercial sources or publicly available data is used by the LEP. The LEP does not have access to such information. The information is retained by the DHS Personnel Security Office or OPM.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the applicant's information is verified directly with the applicant at the beginning of the application process, during the pre-clearance process, and finally by the Personnel Security Division or the OPM investigator during the background check and clearance process.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more information (particularly sensitive PII) may be collected than is necessary to adjudicate an LEP applicant's suitability during the pre-clearance process.

Mitigation: The LEP directs applicant(s) to exclude certain sensitive PII, such as Social Security number, date of birth, and place of birth, from the application process. Only after the applicant has been selected to participate in the LEP, does DHS require the applicant to submit sensitive PII to initiate the requisite background and security clearance investigations. However, the LEP is not privy to this information. The LEP stores all electronic files containing PII submitted during the pre-clearance process[9] in a restricted-access folder on a shared drive.

[9] Pre-clearance for the LEP refers to forms used by the approving offices to determine whether a candidate or candidate's company has a conflict of interest with DHS.

Electronic files containing sensitive PII are password-protected. All hard copy or physical files are stored in locked drawers in secured DHS office space.

Privacy Risk: There is a risk that collecting inaccurate information could result in an unfavorable determination, impacting the applicant's ability to participate in the LEP.

Mitigation: To reduce this risk, the applicant, in coordination with the PSO, has the opportunity to correct erroneous information during the application and pre-clearance process.

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.

Information is used to determine an applicant's suitability to participate in the LEP.

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.

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

Applicants are vetted through the following DHS entities which certify appropriate use of the LEP:

- OCHCO - Appoints LEP applicants who have successfully completed the vetting process as an expert or consultant;
- OGC-GLD - Certifies the proper use of the LEP and ensures all applicant candidate LEP forms are complete and accurate;
- OCPO - Provides procurement information on the private sector employer and advises the LEP on potential conflicts of interest.

- DAEO - Certifies the LEP applicants' OGE 450, identifies conflicts of interest, and advises the participating Component program office on how to avoid conflicts of interest; and
- PSO - Manages the LEP and administers the LEP vetting process.

Once approved by the above entities, the PSO will send the pre-clearance package to the applicable component human capital office to initiate the security clearance process through its normal personnel security procedures. The LEP does not have access to any personnel security determination information.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The LEP acts as a conduit between the requesting Component and the applicant there is a risk of loss or misuse of PII during the routing of documents.

Mitigation: Accordingly, all LEP personnel comply with DHS annual privacy training requirements and are briefed on the proper safeguarding and handling requirements for sensitive PII, to include ensuring access to information is only provided to those with a need-to-know.

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.

LEP applicants are given notice on the Assignment Announcement on the information the PSO collects to determine their qualifications to participate in the LEP. DHS also provides notice in the SORNs listed in Section 1.2 and by the publishing of this PIA.

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

Applying to the LEP is voluntary, and the applicant can opt-out at any time by notifying the Component or PSO of his or her intent to do so. If an individual chooses to opt out of the LEP, and/or leaves the Department, his or her records are removed from the LEP roster, and the associated hard copy records are moved to a separate file that is purged after three years.

Failure to provide sensitive PII, such as SSN, will prevent the applicant from being processed for a security clearance, as OPM requires it to perform a background investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk the LEP applicants, unfamiliar with federal hiring forms and processes, may not understand the Privacy Act notice.

Mitigation: The Privacy Act Notice on the Assignment Announcement and all clearance forms provide notice to applicants about how information will be used. The PSO addresses the criteria with the applicant, if requested. The PSO helps LEP applicants navigate unfamiliar forms and processes during government service on-boarding. The LEP also provides notice with the publishing of this PIA and the SORNs outlined in Section 1.2.

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.

Although the Program began in 2008, DHS did not implement it until January 2012. Information will be obtained in accordance to the approved NARA schedule outlined in Section 1.4 of this PIA.

Initial appointments to the LEP may be made for a period of at least three months and no more than one year. The loaned executive may be reappointed for additional periods with the total appointment not to exceed two years.

Consistent with the limited terms of appointment, all records collected and maintained by the PSO in support of the Loaned Executive Program are covered by the GRS 1 item 17a, and are to be destroyed upon the separation of the employee; except for:

- Ethics determinations regarding the appointment of an unpaid Loaned Executive to DHS (GRS 25 item 3, "destroy 6 years after the waiver or other agreed-upon determination or action has been issued or undertaken or is no longer in effect, whichever is later"); and

- Office of Government Ethics (OGE) Form 450 Confidential Disclosure Report (GRS 25 item 2(b)(2), "destroy when 6 years old; except documents needed in an

ongoing investigation will be retained until no longer needed in the investigation").

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk the PSO does not destroy LEP applicant information when an applicant separates from the LEP.

Mitigation: Most LEP records are destroyed upon separation of the employee (e.g., the end of his or her appointment), unless the records pertain to the loaned executive's ethics determination. The LEP only retains the minimal amount of information necessary and applicants are advised that participation in the LEP is based on their current employment. The individual is responsible to notify DHS if his or her employment changes.

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.

The DHS Personnel Security Office shares information with OPM to process clearance requests, pursuant to the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. Records are maintained at several DHS Headquarters locations and component offices in Washington, DC and field locations; and the Department of Treasury (DTR), Bureau of Public Debt for Office of Inspector General employees and applicants. For background investigations adjudicated by the Office of Personnel Management (OPM), OPM may retain copies of those files pursuant to their records retention schedules.

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

The DHS Personnel Security Office shares information with OPM to process clearance requests, pursuant to the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. This sharing is compatible because the purpose of DHS/ALL-023 is to collect and maintain records of processing of personnel security-related clearance actions, to

record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position.

6.3 Does the project place limitations on re-dissemination?

The DHS Personnel Security Office shares information with OPM to process clearance requests, pursuant to the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. Recipients of any PII collected by the LEP are informed that the information is For Official Use Only/Privacy Act Information and, as such, should not be re-disseminated.

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

The DHS Personnel Security Office shares information with OPM to process clearance requests, pursuant to the DHS/ALL-023 Department of Homeland Security Personnel Security Management SORN. The DHS Personnel Security Office maintains a record of all disclosures outside of the Department in the Integrated Security Management System.[10]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of information being shared beyond the intended scope of the LEP.

Mitigation: Information collected by the LEP program is shared for a limited purpose outside the Department with OPM to process clearance requests. Recipients of any PII collected by the LEP are informed that the information is For Official Use Only/Privacy Act Information and, as such, should not be re-disseminated. When the LEP transmits any lists or information regarding approved private sector individuals, the lists are password-protected, and the password is sent separately. All LEP personnel are required to complete the Department's annual privacy training, and sharing of the information is compatible with the SORNs listed in Section 1.2 of this PIA.

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.

[10] *See* DHS/ALL/PIA-038(a) - Integrated Security Management System (ISMS) PIA, September 16, 2014, *available at* http://www.dhs.gov/publication/dhs-all-pia-038a-integrated-security-management-system-isms.

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

Applicants can access their information during the application, pre-clearance, and clearance process by contacting the PSO. Additionally, an applicant may request information from DHS by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request in writing to the DHS Chief FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528. Further information on the specific requirements of submitting a FOIA/PA request to DHS is available from http://www.dhs.gov/xfoia/editorial_0316.shtm.

The PSO does not maintain records about suitability and security clearances. If an individual want to access records relating to their suitability or security clearance process, they should follow the procedures outlined in DHS/ALL-023 Personal Security Management SORN.[11]

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

Applicants can correct or amend their information during the application, pre-clearance, and clearance process by contacting the PSO. Additionally, an applicant may request information from DHS by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request in writing to the DHS Chief FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528. Further information on the specific requirements of submitting a FOIA/PA request to DHS is available from http://www.dhs.gov/xfoia/editorial_0316.shtm.

The PSO does not maintain records about suitability and security clearances. If an individual want to correct or amend records relating to their suitability or security clearance process, they should follow the procedures outlined in DHS/ALL-023 Personal Security Management SORN.[12]

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

PSO advises applicants of the process for correcting inaccurate information by this PIA, accompanying SORNs, and Privacy Act Statements during the application and subsequent clearance process.

[11] 74 FR 3084, published January 16, 2009.
[12] 74 FR 3084, published January 16, 2009.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that applicants may be unaware of or not understand their redress options.

Mitigation: DHS mitigates this risk by providing applicants with clear notice of their ability to access and correct their information, as well as to seek redress. Applicants are advised of what information is in the custody of the LEP and how to seek redress from those organizations.

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?

Access to information contained in LEP is determined by the role to be performed by the user. Applicable permissions are associated with the role. The information viewed by the privileged or general user is based on the role being performed and the "need to know" principle. Audit trails are reviewed to ensure the appropriate handling of information.

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

All DHS employees and contractors are required to take privacy training annually. The LEP fully complies with the Department's required training.

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

The PSO administers and manages the LEP. PSO shares and provides access to the appropriate officials in DAEO, OGC-GLD, OCPO, and OCHCO, which certifies appropriate use of the LEP.

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?

Not applicable. The LEP does not provide information directly to outside entities. All agreements with OPM are cleared through the DHS Personnel Security Office.

Responsible Officials

Karinda L. Washington
Department of Homeland Security
Private Sector Office

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security