Privacy Impact Assessment
for the

Critical Infrastructure Private Sector Clearance Program

DHS/NPPD/PIA-020

November 2, 2011

Contact Point
Richard LePage
Director of Management
Office of Infrastructure Protection
National Protection and Programs Directorate
(703) 235-8133

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

Abstract

The U.S. Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection sponsors security clearances for certain private sector officials through the Critical Infrastructure Private Sector Clearance Program. These officials are identified through the National Infrastructure Protection Plan (NIPP) partnership framework and are Critical Infrastructure owners/operators, sector leadership (i.e., Sector Coordinating Council members), or subject matter experts identified by DHS to assist in analyzing Critical Infrastructure-related national security information to further enhance the Department's infrastructure protection mission. NPPD conducted this PIA because sponsoring individuals for security clearances involves the collection of PII, such as the applicant's Social Security Number, date and place of birth, and employment contact information.

Overview

Background

Protecting Critical Infrastructure and key resources requires cooperation between government and private industry. It is the policy of the DHS to share pertinent information regarding Critical Infrastructure with the private sector, which at times may include classified information. A private sector official must be cleared for a federal security clearance prior to receiving classified information from the government. The Critical Infrastructure Private Sector Clearance Program (hereinafter referred to as the "Program") was developed to provide a means to facilitate the processing of security clearance applications for private sector partners.

There are three phases to clearance processing: 1) applicant processing; 2) investigation; and 3) adjudication. The Program initiates the applicant processing. However, the U.S. Office of Personnel Management (OPM) and the DHS Office of Security, Personnel Security Division (hereafter referred to as "Personnel Security Division") conduct the background investigation required to obtain a security clearance and the adjudication of the clearance. During Phases Two and Three, OPM or the Personnel Security Division may require additional PII to be collected. This additional information is not shared with the Program, nor stored in the Program system. The Program only collects and retains that information necessary to monitor the status of the individual's clearance processing. Upon adjudication, notification is sent to the Program, who retains the approval. In the event of a denial, only the applicant's name, sector, and date of denial are retained.

Applicant Processing

The Program has identified certain DHS employees, hereafter referred to as Nominators, whose function is to identify specific private sector partners (individuals/applicants) who meet the criteria[1] for sponsorship of a security clearance. Nominators address those individuals in order to seek their

[1] To qualify for Program sponsorship, an individual must meet one of the following criteria: 1) be a member of sector leadership; 2) be a Critical Infrastructure operator/owner or senior corporate official with the authority to effectuate change with respect to Critical Infrastructure; and/or 3) be a subject matter expert.

participation in the Program. If an individual meeting the criteria for sponsorship is interested in becoming part of the Program, the Nominator initiates the applicant processing by providing the individual with the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*.

To minimize the collection of PII, the process is twofold, and sensitive PII is only collected from those individuals who are approved for DHS sponsorship based on information submitted as part of the first step of the clearance application process.

Step one: The applicant must provide the following via DHS Form 9014:

- full name;
- company name;
- business title;
- business physical address;
- business email address;
- business phone number;
- business relationship with the sector;
- U.S. Citizen (yes/no); and
- a justification for the need for access to classified information.

Once the applicant completes and returns the application to the Nominator for their signature, the Nominator forwards the form to the Program's Security Administrator, who reviews it for completeness and initial candidate approval. If the basic application is approved, the Program's Security Administrator contacts the applicant directly to complete the second step, which requires that the individual provide the remaining sensitive PII needed to begin the security clearance process.

Step two: The applicant must provide the following:

- date of birth (DOB);
- place of birth (POB); and
- Social Security Number (SSN).

This two-part process helps minimize the collection of sensitive PII for only those individuals who meet the threshold and are sponsored by DHS.

Upon completion of the initial two-step collection, the Program Security Administrator is responsible for entering the applicant's information into OPM's secure portal for investigation processing, the electronic questionnaire for investigation process (e-QIP[2]). This will initiate the applicant in OPM's system, allowing the applicant to complete OPM's required online security questionnaire. Specifically, the Program Security Administrator enters the following data into e-QIP:

[2] For more information on e-QIP, see OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010).

- name;
- DOB;
- POB;
- Social Security Number; and
- business email address.

Once the Program Security Administrator has initiated the applicant in e-QIP, the applicant accesses e-QIP directly to complete and submit OPM's online security questionnaire, Standard Form 86, *Questionnaire for National Security Positions*. The Program does not collect or have access to the information provided by the applicant to OPM through e-QIP. However, the applicant must provide the Program with copies of e-QIP signature pages that are printed at the end of the security questionnaire, certifying that statements made on the security questionnaire are true, complete, and correct to the best of the applicant's knowledge and that knowingly providing a false statement is punishable by fine or imprisonment or both under 18 U.S.C. §1001.

The applicant's printed e-QIP signature pages are part of a package of DHS forms and standard security forms[3] that must be submitted before the investigation process begins. The forms package also includes a set of fingerprint cards and a DHS Form 11000-9, *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act*. The Program instructs applicants to submit two copies of this package, one in hard copy and one in electronic form. The Program retains the hard copy in the individual's file in a locked filing cabinet, and the electronic copy is password-protected and stored on the Program's access-restricted shared drive. The Program Security Administrator sends the complete, electronic package of forms, fingerprints, including the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, to the Personnel Security Division, via a password-protected email attachment, for processing.

Investigation

The Personnel Security Division reviews the applicant's forms package and performs initial background checks (such as the FBI fingerprint check). Based on the initial review, the Personnel Security Division will either grant or deny an interim security clearance, if appropriate, while OPM conducts a full background investigation.

OPM performs background investigations for all individuals being sponsored by DHS for a security clearance. For more information on OPM's background investigations, see OPM's privacy impact assessment[4] for e-QIP or OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010). Upon completion of the background investigation, OPM sends the investigation file back to DHS for adjudication by the Personnel Security Division. That investigation file is not shared with the Program.

[3] The National Archives and Records Administration, Information Security Oversight Office prescribes standard forms that are used in administering the security classification programs in government.
[4] http://www.opm.gov/privacy/PIAs/eQIP.pdf

Adjudication

The Personnel Security Division evaluates information obtained through the background investigation process and notifies the Program and the applicant of the decision to grant or deny the security clearance via email. In the event that a clearance is denied, the Personnel Security Division also directly advises the applicant in writing of their redress options, to include the ability to access and correct records pursuant to the provisions of the Privacy Act. The Program is only notified of the final decision and does not have access to information used by the Personnel Security Division in its evaluation. In the event of a denial, only the applicant's name, sector, and date of denial are retained.

Individuals who are granted security clearances are required to complete a Standard Form 312, *Classified Information Nondisclosure Agreement*, which serves as contractual agreement between the individual and the United States government, acknowledging the individual's responsibilities inherent with being granted access to classified information. By signing the Standard Form 312, the individual accepts the obligations of being granted access to classified information including, but not limited to, no unauthorized disclosure of such information.

Administrative Security/Classified Visit Management

The Program is further responsible for maintenance of the security clearance, including administering annual training and initiating periodic reinvestigations, as required by Executive Order 12968, as amended,[5] and facilitating classified visit management. The Program maintains a roster to keep track of the individuals' clearance status and shares information, as appropriate, to allow individuals access to classified information for which they have a need to know. To perform these functions, the Program Security Administrator has access to the Department's clearance database managed by the Personnel Security Division, Integrated Security Management System (ISMS), for purposes of verifying clearance status. The use of ISMS for administrative security and classified visit management is covered under the privacy impact assessment, DHS/ALL/PIA-038 Integrated Security Management System (ISMS), published March 22, 2011.

The Program retains the following information, which is collected through the application process and through ISMS:

- In the applicant's file:
  - the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*;
  - the set of fingerprint cards;
  - the DHS Form 11000-9, *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act*; and
  - a copy of the applicant's printed e-QIP signature pages.
- In the Program roster:

[5] Executive Order 12968, as amended, establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

- full name;
- Social Security Number;
- DOB;
- POB;
- sector affiliation;
- date the applicant's package was submitted to the Personnel Security Division;
- date the package was sent to OPM;
- clearance granting date;
- the date the applicant signed their Standard Form 312, *Classified Information Nondisclosure Agreement*;
- their role in their company/sector;
- clearance/nondisclosure agreement/status remarks;
- investigation date;
- clearance level;
- business email address;
- company name;
- business address; and
- business phone number.

Participation in the Program is entirely voluntary. However, failure to provide the required PII may prevent the individual from participating in the Program or receiving a security clearance. Consequently, the individual may not have access to information required to effectively coordinate with the government on Critical Infrastructure matters that are related to national security.

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 and Executive Orders 9397,[6] 12968, 13526,[7] and 13549[8] authorize the collection of this information. Individuals cannot be granted access to classified

[6] Executive Order 9397 gives agencies the authority to collect Social Security Numbers whenever the agency finds it advisable to set up a new identification system for individuals.
[7] Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.
[8] 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,

information unless they have been determined eligible for access based on favorable adjudication of an appropriate background investigation. Additionally, the 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). While the Program does not conduct investigations, the Program 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 Program (i.e., citizenship, Social Security Number, DOB, POB, and standard form questionnaires, etc.) as well as information collected by the Personnel Security Division as part of the investigation and adjudication of the security clearance, is covered under DHS/ALL-023 - Department of Homeland Security Personnel Security Management, 74 FR 3084 (January 16, 2009). The interests of national security require that all persons privileged to access national security information shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. This means that individuals sponsored by DHS for access to classified information are subject to investigation.

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?

The records in this system are covered by the NARA General Records Schedule (GRS) 18 Items 21; 22; 23.

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

The DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, is covered by OMB number 1670-0013.

---

and private sector entities.

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 PII, the process is twofold, and sensitive PII is only collected from those individuals who are approved for DHS sponsorship 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;
- company name;
- business title;
- business physical address;
- business email address;
- business phone number;
- business relationship with the sector;
- U.S. Citizen (yes/no); and
- a justification for the need for access to classified information.

If the individual is deemed suitable for sponsorship, the Program's Security Administrator contacts the applicant directly to complete the second step, which requires that the individual provide the remaining, sensitive PII needed to begin the security clearance process.

Step two: The applicant must provide the following:

- DOB;
- POB; and
- Social Security Number (SSN).

Upon completion of the initial, two-step collection, the Program Security Administrator is responsible for entering the applicant's information into OPM's e-QIP.[9] This will initiate the applicant in OPM's system, allowing the applicant to complete OPM's required online security questionnaire. Specifically, the Program Security Administrator enters the following data into e-QIP:

- name;

[9] For more information on e-QIP, see OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010).

- DOB;
- POB;
- Social Security Number; and
- business email address.

Once the Program Security Administrator has initiated the applicant in e-QIP, the applicant accesses e-QIP directly to complete and submit OPM's online security questionnaire, Standard Form 86, *Questionnaire for National Security Positions*. The applicant provides all information required by OPM to perform its background investigation directly to OPM. The Program does not collect or have access to the information provided by the applicant to OPM through e-QIP. However, the applicant must provide the Program with copies of e-QIP signature pages that are printed at the end of the security questionnaire, certifying that statements made on the security questionnaire are true, complete, and correct to the best of the applicant's knowledge and that knowingly providing a false statement is punishable by fine or imprisonment or both under 18 U.S.C. §1001.

The applicant's printed e-QIP signature pages are part of a package of DHS forms and standard security forms[10] that must be submitted before the investigation process begins. The forms package also includes a set of fingerprint cards, and a DHS Form 11000-9, *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act*.

To initiate the background investigation process, the Program provides the complete package of forms, including the initial DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, to the Personnel Security Division. All other PII required to complete the background investigation and adjudication of the applicant's security clearance is collected by OPM and the Personnel Security Division respectively. The Program does not collect or have access to information obtained by the Personnel Security Division or OPM during the investigation process. Once the background investigation is complete and has been adjudicated by the Personnel Security Division, the Program receives notice of the clearance determination and the date the clearance was granted.

As the Program is responsible for maintenance of the security clearance, including administering annual training and initiating periodic reinvestigations, the Program maintains a roster to track the status of individuals' security clearances. That roster includes the following information: full name, Social Security Number, DOB, POB, sector affiliation, date the applicant's package was submitted to the Personnel Security Division, date the package was sent to OPM, clearance granting date, the date the applicant signed their Standard Form 312, *Classified Information Nondisclosure* Agreement, their role in their company/sector, clearance/nondisclosure agreement/status remarks, investigation date, clearance level, email address, company name, business address, and business phone number.

[10] The National Archives and Records Administration, Information Security Oversight Office prescribes standard forms that are used in administering the security classification programs in government.

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

All information that the Program collects as part of the clearance application process (e.g. forms, fingerprint cards, and a copy of the applicant's printed e-QIP signature pages) are submitted to the Program directly from the applicant. Applicants are directed to provide information to the Program both in hard copy and in electronic form. Applicants provide hard copy documents to the Program via regular mail while electronic documents are provided to the Program via password-protected e-mail attachments.

The only information the Program receives that does not come directly from the applicant is the administrative tracking information (e.g., date the package was sent to OPM, date the applicant's clearance was granted) and the notification of determination from the Personnel Security Division. The Program Security Administrator also has access to the Department's clearance database managed by the Personnel Security Division, Integrated Security Management System (ISMS) for the purpose of verifying individuals' clearance status to ensure the Program roster of cleared partners remains current. For information on ISMS, please review the privacy impact assessment, DHS/ALL/PIA-038 Integrated Security Management System (ISMS).

The individual has a direct relationship with OPM and provides all information required in support of OPM's background investigation directly to OPM via the Standard Form 86, *Questionnaire for National Security Positions*, which the applicant submits through OPM's secure portal for investigation processing, e-QIP. For more information on e-QIP, see OPM's privacy impact assessment[11] or OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010). The Program does not collect or have access to the information provided by the applicant to OPM through e-QIP.

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 OPM or the Personnel Security Division in support of their background investigations (e.g., to perform credit checks), the Program does not have access to such information. No commercial sources or publicly available data is used by NPPD or the Program. The Program only collects and retains information in support of its sponsorship function, and all information collected is provided voluntarily by the individual.

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 clearance process, by the Program Security Administrator, and during the investigation, by the Personnel Security Division or OPM investigator. Additionally, the Program Security Administrator,

[11] http://www.opm.gov/privacy/PIAs/eQIP.pdf

who has access to ISMS, verifies the investigation/clearance information with the ISMS clearance database.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that an individual may be unaware that he/she has been nominated for sponsorship of a security clearance.

Mitigation: This risk is mitigated in that the Program collects information directly from the applicant as part of the nomination process and is further mitigated in that the application process is twofold, and sensitive PII is only collected from those individuals who are approved for DHS sponsorship based on information submitted as part of the first step of the clearance application process..

Privacy Risk: There is a privacy risk that more information (particularly sensitive PII) than is necessary may be collected.

Mitigation: This risk is mitigated in that the Program's policy is to direct the applicant to exclude certain sensitive PII, such as Social Security Number, DOB, and POB, from the initial clearance request application until the Program's Security Administrator has approved the applicant to be sponsored by DHS for a security clearance. Only after that initial approval does the applicant provide the remaining, sensitive PII necessary to initiate the requisite background investigations. The Program stores all electronic files containing PII in a restricted-access folder on a shared drive. Electronic files containing sensitive PII are password-protected. All hard copy or physical files are stored in locked drawers in secured DHS office space. Only the Program Security Administrator has the keys to those drawers.

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

Mitigation: To reduce this risk, the Program collects information required as part of the application process directly from the applicant. The applicant also has a direct relationship with the Personnel Security Division and with OPM through e-QIP and has the opportunity to correct erroneous information during the investigation 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.

The Program collects information from private sector partners in order to sponsor those individuals for security clearances so that DHS may share pertinent information regarding infrastructure protection, which at times may include classified information. For example, an individual would need a

security clearance in order to attend a classified meeting or briefing in which Critical Infrastructure information is being shared.

Specifically, the Program uses information obtained during the security clearance process in support of the following functions: to initiate a background security investigation; verify identity; grant physical access to a facility; grant a security clearance; confirm an applicant's clearance status via ISMS; communicate security updates; send meeting invites; conduct briefings; share sanitized contact lists, as appropriate, with DHS cleared officials (e.g., Sector Specialists, Protective Security Advisors, etc.); or to perform other security activities or general communications.

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, the Program does not utilize technology to analyze the data in any way.

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

The clearance process is initiated by the Program and completed by the Personnel Security Division. No other DHS components are involved unless the applicant previously held a reinstateable clearance with another DHS component. For example, if an applicant is a former cleared U.S. Secret Service employee and is within the two-year window of reinstating their clearance, the Personnel Security Division will contact the U.S. Secret Service to obtain the individual's previous investigative file.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: As the Program acts as a liaison between the applicant and the Personnel Security Division, there is a risk of loss or misuse of PII while the clearance request application and other documents are being routed for signature or further processing.

Mitigation: This risk is mitigated in that the Program limits the collection of most sensitive PII to those individuals who receive initial approval for DHS sponsorship from the Program's Security Administrator. Additionally, all Program 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. This risk is fully mitigated in that the Program instructs individuals who must provide sensitive PII to do so via password-protected e-mail attachments. Passwords are sent via separate email to further minimize this risk should an email be inadvertently misdirected. When the Program forwards information to the Personnel Security Division, the same protections remain in place.

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.

The Program provides notice at the point of collection via a Privacy Act statement on the DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*. This statement advises the individual as to how their information will be used and why it is needed. Additionally, DHS provides notice in the form of this PIA and the system of records notice for DHS/ALL-023 - Department of Homeland Security Personnel Security Management, 74 FR 3084 (January 16, 2009).

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

Providing information to the Program is voluntary, and the individual can opt out at any time by notifying the Nominator or Program Security Administrator of their intent to do so. If an individual chooses to opt out of the Program, and/or leaves the Department, after having started or completed the clearance process, their records are removed from the Program 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 Social Security Number, would prevent the individual from being processed for a security clearance, as that is required by OPM to perform its background investigation.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the notice provided may be inadequate.

Mitigation: This risk is mitigated in that the Program provides notice to ensure that Program applicants are aware of how their information is being used. Participation in the Program is completely voluntary, and Nominators address the criteria for sponsorship with each applicant upon expressing interest in becoming part of the Program. The Program provides notice in this PIA and the SORN. OPM also provides notice applicable to the collection of information through e-QIP.

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.

In accordance with the Personnel Security Division's procedures, the Program maintains the applicant's clearance information both in a secured folder on the shared drive and in a physical file in a locked drawer, with access limited to only those that have a need to know. The Program maintains certain information pertaining to the individual's clearance status on a clearance roster, which is also maintained in a secure folder on the shared drive. The records retention schedule is covered by the NARA General Records Schedule (GRS) 18 Items 21; 22; 23. Records are maintained from the time an applicant begins the clearance application process until their security clearance is deactivated or the individual's participation with the Program is terminated. Destruction of an individual's record will occur upon notification of death or not later than five years after separation or transfer of employee or no later than five years after contract relationship expires, whichever is applicable. Individuals who no longer require access to classified information are removed from the roster, and their records are moved to a separate drawer and purged after three years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Applicants covered by the Program are private sector individuals whose DHS sponsorship is based on their relationship with DHS and need for access to classified information at the time of their nomination to the Program. There is a risk that the Program may retain information longer than necessary where an applicant separates from the Program or no longer requires access to classified information.

Mitigation: The Program only retains the minimal amount of information necessary to perform routine security activities, such as verifying clearance status or granting access to a facility. This risk is fully mitigated in that applicants are advised that the Program's sponsorship is based on their current employment, and the individual is responsible to notify DHS if their employment changes, in which case the program would re-evaluate their need for access to classified information. Additionally, the Program continually updates its roster to ensure that only current and relevant information is maintained. The Program Security Administrator has access to ISMS, the clearance database maintained by the Personnel Security Division, in order to verify an individual's clearance status. If access to classified information is revoked, the individual's information is purged in accordance with the GRS.

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 Program shares limited information with OPM in order to initiate the applicant in e-QIP where the applicant completes OPM's online security questionnaire, Standard Form 86, *Questionnaire for National Security Positions*. To initiate the applicant, the Program Security Administrator enters the following data into e-QIP:

- full name;
- DOB;
- POB;
- Social Security Number; and
- business email address.

The Program may at times share lists of cleared individuals with external federal agencies to facilitate clearing those individuals for participation in classified communications hosted by agencies other than DHS. For example, in order for our financial sector partners to participate in a classified briefing from the Department of Treasury, the Program would need to share a list of those partners who hold security clearances with the Department of Treasury. The Program would accomplish this by extracting relevant information from its clearance roster, sanitizing the list, to remove any sensitive PII, and sharing information pertaining only to those individuals who require access to the classified briefing. The sanitized list would include:

- full name;
- company name;
- city;
- state; and
- business email address.

While the Program is responsible for compiling lists of cleared partners to facilitate classified briefings, the Program does not share any sensitive PII outside of DHS. Where sensitive PII or other information is required to verify an individual's security clearance, the Personnel Security Division is responsible for passing the information to the external agency.

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

The Program only shares information outside of DHS to allow external agencies to confirm the individual's clearance status when access to classified information is required. This sharing is compatible with the routine uses published in DHS/ALL-023 - Department of Homeland Security Personnel Security Management, 74 FR 3084 (January 16, 2009).

6.3 Does the project place limitations on re-dissemination?

If any participant's information is shared with external agencies, the information is marked as For Official Use Only (FOUO)/Privacy Act Information, and the recipient is notified not to further disseminate.

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

The Program keeps both paper and electronic records of external sharing. There is a log of external requests that have been made along with email communication regarding the dissemination.

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 Program.

Mitigation: Recipients of any PII collected by the Program are informed that the information is FOUO/Privacy Act Information and, as such, should not be re-disseminated. When the Program transmits any lists or information regarding cleared private sector individuals, the lists are password-protected, and the password is sent separately. All Program personnel are required to complete the Department's annual privacy training, and sharing of the information is compatible with the Department's published SORN.

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?

While the Program collects information at the initial stages of the application, the Personnel Security Division maintains the official security file for the individual. The Personnel Security Division advises clearance applicants of their clearance status via email notification, to include advising them of

the procedures for requesting access to their information under the provisions of the Privacy Act. An individual may request information from DHS by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to the DHS 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.

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

Once OPM initiates its background investigation, OPM works directly with the applicant, providing that individual with the opportunity to correct inaccurate or erroneous information. Once the clearance process is complete and has been adjudicated by DHS, the individual can correct erroneous information in DHS's records by submitting a request to the DHS FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528. For any information that is under the control of OPM, the individual would need to contact OPM directly.

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

The Program advises applicants of procedures for correcting their information in various ways throughout the application process. First, applicants are advised of the procedures during the nomination and initial application processes. Second, OPM's e-QIP system has built-in mechanisms for identifying erroneous information. For example, if the applicant is unable to log into e-QIP, this generally indicates that the information the Program Security Administrator inputted into e-QIP to initiate the applicant's security clearance questionnaire was entered incorrectly. The e-QIP system prompts users to contact their agency point of contact for assistance with log-in help. In such instances, the applicant is instructed to contact the Program Security Administrator who works with the applicant to correct any erroneous information. The Program Security Administrator also instructs applicants to print out a review copy of their e-QIP form to verify the accuracy of their responses before finalizing them. Lastly, the e-QIP system provides error messages when information is missing or entered incorrectly, which prompts the user to address the error before the user is able to submit information for processing.

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: This risk is mitigated in that the Program provides individuals 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 Program and what information is maintained with the Personnel Security Division or with OPM respectfully, 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?

The Program has undergone Site Assistance Visits by the Privacy Office in the past, as well as by the Office of Security Administrative Security Division (December 2009). The Program has also met with the Inspector General's Office (December 2010). Access restrictions to the physical and electronic files do not change unless a new employee or contractor begins work on the Program.

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 Act training annually. The Program 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?

Only the Program Security Administrator and staff directly supporting the Program have direct access to the physical and electronic files. The Program only shares information for the purpose of facilitating the clearance application processing and for classified visitor management. When information is requested, the requestor's "need-to-know" is reviewed, and if approved by the Program Security Administrator, the Program shares only that information required to fulfill a specific purpose. For example, a state-specific list of clearance holders may be required to facilitate a classified briefing for private sector partners. If approved by the Program Security Administrator, the Program would share a password-protected list of clearance holders, sanitized of sensitive PII, with the agency hosting the briefing. This list would typically include: full name, sector, clearance level, company name, role in company, their location (city/state), and business email address.

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?

The Program does not currently have any information sharing agreements or MOUs for sharing data with other organizations.

Responsible Officials

Richard LePage
Director of Management
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