Privacy Impact Assessment Update
for the

Private Sector Clearance Program for Critical Infrastructure

DHS/NPPD/PIA-020(a)

February 11, 2015

Contact Point
Tonya Schreiber
Director, Sector Outreach and Programs Division
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
(703) 603-5087

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

Abstract

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD) is updating the Private Sector Clearance Program for Critical Infrastructure's (PSCP) Privacy Impact Assessment (PIA) to account for changes to the program since the publication of the program's original PIA on November 2, 2011.

Overview

Protecting critical infrastructure security and resilience requires ongoing cooperation between Government and private industry. While the vast majority of information DHS shares with the private sector is at the unclassified level, some information may be classified, requiring a federal security clearance. The Private Sector Clearance Program for Critical Infrastructure (PSCP), established in 2006, ensures that critical infrastructure private sector owners, operators, and industry representatives, specifically those in positions responsible for the protection, security, and resilience of their assets, are processed for the appropriate security clearances. With clearances, these owners, operators, and representatives can access classified information to make more informed decisions. The PSCP facilitates the processing of security clearance applications for private sector partners, and is currently administered by the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP), Sector Outreach and Programs Division (SOPD).

Reason for the PIA Update

This PIA Update addresses specific updates and improvements that NPPD/IP has made to the PSCP since the program's original PIA was published on November 2, 2011. Updates include:

- Enhancements made to the PSCP to meet the intent of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*;[1]
- Changes made to roles and responsibilities under the PCSP, specifically the elimination of the Program Security Administrator role and the delegation of those responsibilities to the new PSCP Administrator and designated specialists within the IP Security Office;
- The collection of additional data elements from qualified[2] individuals (Nominees)

[1] Exec. Order No. 13636, 77 FR 11739 (Feb. 19, 2013).
[2] *See* Exec. Order No. 13549 § 5(g), 75 FR 51609 (Aug. 18, 2010). Individuals eligible to participate in the PSCP include: 1) Corporate owners and operators determined by the Secretary of Homeland Security to be part of the Critical Infrastructure or Key Resources (CIKR); 2) Subject matter experts selected to assist the federal or state CIKR; 3) Personnel serving in specific leadership positions of CIKR coordination, operations, and oversight; 4) Employees of corporate entities relating to the protection of CIKR; and 5) Other entities involved in public safety or related activities that support the security of our communities and the Nation, but who are not otherwise eligible for

who require clearances based on their day-to-day work related to the security and protection of critical infrastructure through the updated DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*; and

- The implementation of the Homeland Security Information Network-Critical Infrastructure (HSIN-CI)/PSCP Website, which was developed as a security clearance management tool.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*

EO 13636,[3] issued in February 2013, directed federal departments and agencies to work together and with the private sector to strengthen the security and resilience of the Nation's critical infrastructure. Section 4(d) of the EO specifically directs DHS to "expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in Section 9 of this Order." Section 9 further requires the Secretary to identify critical infrastructure in which a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

In order to effectively meet the requirements outlined in Section 4(d) of the EO, as well as other critical needs for clearances, the Department developed three categories to prioritize private sector clearance applicants. DHS assigns the applicant's priority category during the initial application phase. The applicant's priority category remains throughout the clearance package until DHS makes a clearance determination for the applicant. The three categories of prioritization are:

1. **Normal Prioritization**- This is the default categorization for clearance applications;
2. **Time-Critical Prioritization**- This is an accelerated process in which the application sponsor[4] has certified a near-term threat requiring a security clearance and a pending classified threat briefing to share that information; and
3. **Expedited Prioritization**- This is the fastest option and applies to applications for personnel of critical infrastructure owners and operators, in which "a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," as identified in Section 9 of EO 13636.

Applications designated as Time-Critical or Expedited will receive priority processing at each

---

the granting of a personnel security clearance pursuant to EO 12829, as amended.

[3] Exec. Order No. 13636, 77 FR 11739 (Feb. 19, 2013).

[4] Sponsors are the organizations sponsoring the security clearance. DHS, a Sector Specific Agency, or another federal department or agency may sponsor a security clearance through the PSCP, depending on who is seeking to share the information with the private sector.

phase of the application process.

PSCP Roles and Responsibilities

Since the original PSCP PIA was published, DHS eliminated the role of the Program Security Administrator. As the PSCP has continued to grow, DHS split the Program Security Administrator role between the new PSCP Administrator position within IP/SOPD and designated security specialists within the IP Security Office.

Previously, the Program Security Administrator handled the administrative processing and initial approval of DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, as well as contacted Nominees to collect their sensitive personally identifiable information (PII), entered Nominee information into the Office of Personnel Management's (OPM) secure portal for investigative processing, the Electronic Questionnaire for Investigations Processing (e-QIP),[5] and worked with the DHS Office of the Chief Security Officer (OCSO). Now, the PSCP Administrator is responsible for the administrative processing and routing of DHS Form 9014 to the Office of the Assistant Secretary (OAS) for IP for approval. Designated security specialists within the IP Security Office collect the Nominee's sensitive PII, enter Nominee information into e-QIP, and work with DHS OCSO. These changes in roles and responsibilities further ensure that the sharing of sensitive PII is limited to only those who have a need to know, as a Nominee's sensitive PII is only accessible to the designated IP Security Office specialists tasked with collecting the information. The PSCP Administrator role does not have access to any of the Nominees' sensitive PII. The updated PSCP clearance process, which accounts for these changes, is outlined below.

PSCP Clearance Process

As described in the November 2011 PIA, the processing of federal security clearances for the PSCP consists of three phases: (1) applicant processing; (2) investigation; and (3) adjudication. OPM and OCSO are responsible for phases two and three.

Applicant Processing

Sector Specific Agencies,[6] Protective Security Advisors, DHS IP Sector Liaisons, the National Infrastructure Coordinating Center, and other federal officials designated by DHS IP (Nominators), identify qualified Nominees who require clearances based on their day-to-day

[5] For more information on OPM's background investigations, *see* OPM's privacy impact assessment for e-QIP, *available at* http://www.opm.gov/privacy/PIAs/eQIP.pdf. *See also* OPM/CENTRAL-9 - Personnel Investigation Records, 75 FR 28307 (May 20, 2010).

[6] A Sector Specific Agency is a federal department or agency designated under Presidential Policy Directive-21 (PPD-21) to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. *See* PPD-21, *Critical Infrastructure Security and Resilience*, February 12, 2013.

work related to the security and protection of critical infrastructure. Nominators then contact identified Nominees to seek their participation in the PSCP. If a Nominee is interested in becoming part of the PSCP, then the Nominator initiates the applicant processing by providing the Nominee with DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request.* Since the original PSCP PIA was published in November 2011, DHS Form 9014 has been updated to request additional data elements from PSCP Nominees in order to improve the program's overall effectiveness. These new data elements are denoted by an (*) in the two-step collection process outlined below.

In order to minimize the collection of sensitive PII, the PSCP employs a twofold collection process, which allows sensitive PII to be collected only from those Nominees who are approved for DHS sponsorship based on information submitted as part of the first step of the clearance application process.

Step one: The Nominee must provide the following information via the updated DHS Form 9014 *(Note: (*) denotes a new data element requested on the updated DHS Form 9014)*:

- Full name;
- Company name and address;
- Business phone number;
- Business email address;
- Level of clearance requested;
- Current association memberships;
- U.S. Citizen (yes/no);
- Justification to access classified information (to include Nominee's job title, position, and responsibilities);
- Information regarding whether the Nominee's company Chief Security Officer (or the executive otherwise responsible for the Nominee organization's security posture) has been notified of the Nominee's nomination (yes/no/N/A);*
- Information regarding whether there is a secure facility within 50 miles where clearance holder may attend a classified briefing (yes/no/no, but willing to travel);*
- Information pertaining to how the Nominee satisfies the criteria for PSCP nomination (checkboxes provide the criteria selection from EO 13549[7]);* and
- Nominee's sector.

[7] *See* Exec. Order No. 13549, 75 FR 51609 (Aug. 18, 2010).

If the Nominee has held an active clearance within the past 24 months, then the Nominee must also provide:

- Whether he or she previously held or currently holds a clearance and what type of clearance he or she held or holds (Secret/Top Secret);
- The name of the Agency that sponsored the clearance;
- Contact information for his or her Security Official/Office (phone number and email address);
- Information regarding whether he or she is retired or separated or if he or she is planning on retiring and separating from the position in which he or she held an active clearance within the past 24 months (to include from where the Nominee is retiring or separating);
- If the Nominee is retired or separated, then he or she must also provide his or her date of retirement or separation;
- Reciprocity/reinstatement (yes/no (Nominees may only select "yes" if they have a current clearance or if their prior security clearance was active within the last 2 years));* and
- If a PSCP clearance holder is undergoing a reinvestigation, then he or she must provide information regarding how recently he or she used the PSCP clearance (No, Yes-within the past year, Yes-within the past 2 years, Yes-within the last 5 years, or Yes-within the last 10 years).*

Once the Nominee completes and returns DHS Form 9014 to the Nominator for his or her signature, the Nominator forwards the form to the PSCP Administrator. The PSCP Administrator then reviews the form to ensure completeness, validate Nominee eligibility, validate the criteria justifying the clearance, and identify the priority level of the request to meet the intent of EO 13636. At this time, the PSCP Administrator also logs the Nominee's name, contact information, job title, and justification into a SharePoint database maintained through the HSIN-CI[8] prior to submitting the Nominee's information to IP's OAS for approval. This SharePoint database resides on a specific PSCP site within HSIN-CI and serves as a security clearance management tool. Access to this HSIN-CI/PSCP site is restricted to Nominators and authorized DHS employees that work within the PSCP. No sensitive PII is maintained within this database.

If the OAS does not approve the nomination or requests further justification prior to processing, the OAS returns the Nominee's DHS Form 9014 to the PSCP Administrator. The PSCP Administrator notifies the Nominator of the need for additional information or non-concurrence and rationale. As the Nominee's primary point of contact, the Nominator then

[8] For more information on HSIN-CI, *see* DHS/OPS/PIA-002-Homeland Security Information Network (HSIN) Sensitive But Unclassified (SBU), *available at* www.dhs.gov/privacy.

informs the Nominee of the OAS's need for additional information or non-concurrence and rationale.

If approved by the OAS, then the OAS submits the Nominee's DHS Form 9014 to the IP Security Office for further processing and submission to DHS OCSO. IP Security contacts the Nominee directly to complete the second step, which requires that the Nominee provide the sensitive PII needed to begin the security clearance process.

Step two: The Nominee must provide the following *(Note: (*) denotes a new data element requested on the updated DHS Form 9014)*:

- Date of birth (DOB);
- Place of birth (POB);
- Social Security number (SSN); and
- Mailing address (optional)*- Nominees have the option to submit an alternative mailing address, since their company's mailing address is sometimes different from the Nominee's physical work address. Since these address discrepancies sometimes create problems when DHS attempts to mail information to Nominees, DHS provides Nominees with an alternative mailing address option.

The information collected for step two is only available to the Security Specialist within the IP Security Office working with the PSCP. DHS retains the Nominee's information in the Integrated Security Management System (ISMS),[9] which is maintained by OCSO.

Upon completion of the initial two-step collection, the IP Security Office enters the Nominee's information into OPM's e-QIP system. This initiates the Nominee in OPM's system, allowing the Nominee to complete OPM's required online security questionnaire. Specifically, the IP Security Office enters the following data into e-QIP:

- Name;
- DOB;
- POB;
- SSN; and
- Business email address.

Once the IP Security Office has initiated the Nominee in e-QIP, the Nominee accesses e-QIP directly to complete and submit OPM's online security questionnaire, Standard Form 86, *Questionnaire for National Security Positions*. The PSCP does not collect or have access to the information provided by the Nominee to OPM through e-QIP. However, the Nominee must provide the IP Security Office with copies of the e-QIP signature pages that are printed at the end

[9] *See* DHS/ALL/PIA-038(a) - Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.

of the security questionnaire, certifying that statements made on the security questionnaire are true, complete, and correct to the best of the Nominee's knowledge and that knowingly providing a false statement is punishable by fine or imprisonment or both under 18 U.S.C. § 1001.

The Nominee's printed e-QIP signature pages are part of a package of DHS forms and standard security forms[10] that must be submitted to OCSO 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 IP Security Office instructs Nominees to submit two copies of this package, one in hardcopy and one in electronic form. The IP Security Office retains the hardcopy of the forms package in the individual's file in a locked filing cabinet, and the electronic copy is password-protected and stored on an access-restricted shared drive. The IP Security Office sends the complete, electronic package of forms and fingerprints, including DHS Form 9014, to OCSO via a password-protected email attachment for processing.

Investigation

OCSO conducts the preliminary background checks and initiates a background investigation with OPM. OPM performs background investigations for all individuals being sponsored by DHS for a security clearance. Upon completion of the background investigation, OPM sends the investigation file back to DHS for adjudication by OCSO. OPM and OSCO do not share the investigation file with the IP Security Office or the PSCP Administrator.

Adjudication

OCSO evaluates information obtained through the background investigation process and notifies the PSCP and the Nominator of its decision to grant or deny the security clearance via email. In the event that a clearance is denied, OCSO also directly advises the applicant in writing of his or her redress options, which includes accessing and correcting records pursuant to the provisions of the Privacy Act of 1974, as amended. The PSCP is only notified of the final decision and does not have access to information used by OCSO in its evaluation. In the event of a denial, the PSCP retains only the applicant's name, sector, and date of denial in a secured folder on a shared drive as well as in a physical file in a locked drawer, with access limited to only those that have an official need to know.

Those Nominees who are granted security clearances (clearance holders) must 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

[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.

classified information including restrictions on disclosing classified information without authorization.

Administrative Security/Classified Visit Management

The PSCP is further responsible for facilitating classified visit management by tracking the status of PSCP Nominee and clearance holder information so that the PSCP may provide PSCP clearance holders with access to classified information for which they have a need-to-know. In the PSCP PIA published in November 2011, the Program Security Administrator performed these functions by accessing ISMS. This role is now carried out by designated IP Security Office Specialists working with the PSCP.

Homeland Security Information Network-Critical Infrastructure (HSIN-CI)/PSCP Website

SOPD has developed a specific PSCP website within HSIN-CI to act as a security clearance management tool. This site is used to maintain information received by the PSCP Administrator from IP Security on both PSCP clearance holders as well as PSCP Nominees. Nominators and authorized DHS employees are granted read-only access to view information maintained on this site for official use only in order to execute the mission of infrastructure protection. Prior to the development of this HSIN-CI/PSCP website, the PSCP Administrator provided a monthly Excel Spreadsheet to Nominators and authorized DHS employees, which was specific to their individual region or sector. Since many of the sectors overlap, federal Nominators and authorized DHS employees require information about clearance holders across sectors and regions. For example, within IP, the Energy Sector is split between the Oil and Natural Gas, Electric, and Nuclear sectors. Providing Energy Sector users with the full picture across all energy sectors, instead of just selecting one, increases their situational awareness. Through the new HSIN-CI/PSCP site, Nominators will have the ability to view clearance holder information across all regions, which helps ensure that they are nominating an appropriate number of individuals across sectors. Providing this data in an electronic read format also decreases the level of risk for data spills that commonly occur when information is transmitted by email.

The HSIN-CI/PSCP site maintains only non-sensitive PII on PSCP clearance holders and PSCP Nominees that IP Security has access to through ISMS. For clearance holders that hold any level of clearance through the PSCP, the HSIN-CI/PSCP site maintains the following information: first and last name, clearance level, sector, company, job title, work location city and state, work email, and work phone number. The site maintains the same information on PSCP Nominees, except that it also captures their clearance process status (i.e., waiting for additional PII from Nominee, waiting for e-QIP, submitted to the OCSO) and their PSCP Nominator's name.

The HSIN-CI/PSCP site allows the PSCP Administrator to restrict site access and controls to ensure only Nominators and authorized DHS employees (users) have access to PSCP

information. Users within the HSIN-CI/PSCP site do not have the ability to change or manipulate data housed on the site. Access to HSIN-CI/PSCP is role-based, which allows the administrator to limit user capabilities to "read-only." All areas that are open to users will be read-only except the document library. The document library houses policy documents, outreach material, forms, metrics reports, and other similar types of documents that do not contain any PII.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

EO 13636, *Improving Critical Infrastructure Cybersecurity*, Section 4(d), requires the Secretary, as the Executive Agent for the Classified National Security Information Program created under EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, to expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in Section 9 of the EO. Section 9 requires the Secretary to identify critical infrastructure in which a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. DHS employed the PSCP to meet this objective and other critical needs for clearances, adjusting processes and criteria to meet the requirements of EO 13636.

The HSIN-CI/PSCP site is certified and accredited through the HSIN-CI system until June 2015.

DHS Form 9014, *Critical Infrastructure Private Sector Clearance Program Request*, was recently updated and is currently going through the Paperwork Reduction Act (PRA) process. The form has not yet received an Office of Management and Budget (OMB) Control Number.

Characterization of the Information

With the enhancements to the PSCP, NPPD/IP is expanding the categories of information collected. DHS Form 9014 is being updated to request the additional data elements from PSCP Nominees listed above. The new data elements are being added to improve the program's overall effectiveness. For example, the PSCP is now requesting that Nominees provide information regarding whether or not they are located within 50 miles of a secure facility for classified briefings. This information will help the program determine the best way to deliver classified information to the PSCP Nominee if and when he or she is provided with a clearance. Furthermore, the updated DHS Form 9014 requests information from PSCP clearance holders undergoing reinvestigations regarding how often they have used their federal security clearance. This information will provide the PSCP with a better understanding of whether a clearance

holder should continue to hold a federal security clearance in order to perform his or her duties.

Privacy Risk: There is a privacy risk that DHS may collect more information than is necessary as a result of the updated DHS Form 9014.

Mitigation: This risk is partially mitigated by the fact that the new data fields on the updated DHS Form 9014 request only non-sensitive PII from PSCP Nominees. This risk is further mitigated by the two-step collection process, which allows sensitive PII to be collected only from those Nominees who are approved for DHS sponsorship based on the information submitted as part of the first step of the clearance process.

Uses of the Information

This HSIN-CI/PSCP site is used to maintain information received by the PSCP Administrator from IP Security on both PSCP clearance holders as well as Nominees. Nominators and authorized DHS employees are granted read-only access to view information maintained on this site to perform official duties.

Privacy Risk: With the development of the HSIN-CI/PSCP site, there is a privacy risk that individuals outside of the PSCP could access and manipulate PSCP clearance holder/Nominee information.

Mitigation: This risk is mitigated by several factors. First, HSIN is a secure system and access to communities of interest, such as HSIN-CI, are granted by invitation only. Secondly, the PSCP Administrator restricts site access and controls to ensure only Nominators and authorized DHS employees have access to PSCP information. Furthermore, users within the HSIN-CI/PSCP site do not have the ability to change or manipulate data maintained on the site as access is role-based, which allows the administrator to limit user capabilities to read-only access. Lastly, the risk is mitigated by the fact that the information maintained on the HSIN-CI/PSCP site is minimized to include only non-sensitive information.

Privacy Risk: Users of the HSIN-CI/PSCP site will have increased access to PSCP clearance holder and Nominee information across all regions and sectors, which may result in the user accessing information for which he or she does not have a need to know.

Mitigation: This risk is mitigated because access to the HSIN-CI/PSCP site is restricted to Nominators and authorized DHS employees with a verifiable need to know. In order to gain access to the HSIN-CI/PSCP site, potential users must first be invited to the HSIN-CI community of interest (COI) via the HSIN nomination and validation process. HSIN-CI is a collection of portals established to support and encourage information sharing in the critical infrastructure COI. Upon accepting this invitation, potential users submit biographical information and employment information so that they may be verified as legitimate members of

the critical infrastructure COI.[11] Once verified, the user is given access privileges to the HSIN-CI COI. Access to HSIN-CI is only the first step, however, as access to the HSIN-CI/PSCP website is further restricted to only those HSIN-CI users that are federal Nominators or authorized DHS employees invited to access the HSIN-CI/PSCP site by the PSCP Administrator. This two-step process ensures that the HSIN-CI/PSCP website is accessed only by members of the critical infrastructure community that are PSCP Nominators or authorized DHS employees with an official need to know.

Notice

No change from the November 2011 PIA.

Data Retention by the project

No change from the November 2011 PIA.

Information Sharing

Since the last PIA was published, the PSCP has enhanced its internal information sharing by developing the HSIN-CI/PSCP site. The site will be used to maintain information received by the PSCP Administrator from IP Security on both PSCP clearance holders as well as Nominees. Nominators and authorized DHS employees will be granted access to view information maintained on this site to perform their required duties of working with these clearance holders and Nominees to execute the mission of infrastructure protection.

Privacy Risk: With the development of the HSIN-CI/PSCP site, there is a privacy risk that PSCP clearance holder and Nominee information could be shared inappropriately outside of the PSCP.

Mitigation: This risk is mitigated by having the program maintain only a sanitized version (containing no sensitive PII) of PSCP clearance holder and Nominee information on the HSIN-CI/PSCP site. In addition, the PSCP Administrator restricts site access and controls to ensure only Nominators and authorized DHS employees have access to PSCP information. Users within the HSIN-CI/PSCP site do not have the ability to change or manipulate data housed on the site. Furthermore, access to the HSIN-CI/PSCP site is role-based, which allows the administrator to limit user capabilities to read-only.

Redress

No change from the November 2011 PIA.

[11] *See* DHS/OPS/PIA-002 - Homeland Security Information Network (HSIN) Sensitive But Unclassified (SBU), *available at* www.dhs.gov/privacy.

Auditing and Accountability

No change from the November 2011 PIA.

Responsible Official

Tonya Schreiber
Director, Sector Outreach and Programs Division
Office of Infrastructure Protection, National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security