Privacy Impact Assessment Update
for the

Private Sector Clearance Program for Critical Infrastructure

DHS/NPPD/PIA-020(b)

April 20, 2018

Contact Point
Cynthia Briscoe
Branch Chief, Security Office
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security
(703) 235-8177

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1664

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 PSCP clearance process and to the DHS Form 9014, *Private Sector Clearance Request Form*. DHS is updating and replacing the PIA, last published in March 2018 to remove references to the Cooperative Research and Development Agreement and the Classified Critical Infrastructure Protection Program because such references were also removed from the newly renamed DHS Form 9014, *Private Sector Clearance Request Form*.

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 these security clearance applications for private sector partners, and is currently administered by the DHS NPPD Office of Infrastructure Protection (IP) Security Office.

Reason for the PIA Update

This PIA Update addresses changes that NPPD/IP has made to the program since the publication of the February 11, 2015, PIA Update. Updates include:

- Clarification of the role that PSCP now plays in the clearance process for private sector partners across NPPD;
- The collection of additional data elements through DHS Form 9014, the updated version of which is called the *Private Sector Clearance Request Form*, from applicants who require clearances based on their day-to-day work related to the security and protection of critical infrastructure; and
- Removal of the Homeland Security Information Network – Critical Infrastructure (HSIN-CI)/PSCP Website, which was never implemented or used.

PSCP Clearance Process Update

A central PSCP Administrator within the IP Security Office receives PSCP requests and processes application packages. Sector Specific Agencies (SSA), Protective Security Advisors (PSA), DHS IP Sector Liaisons, the National Infrastructure Coordinating Center, and other federal officials designated by DHS NPPD may serve as Nominators of private sector security clearance requests. Nominators identify Subjects for nomination and formal sponsorship for a Secret clearance. The Nominator works with the Subject to complete the DHS Form 9014. The completed form is forwarded to the PSCP Administrator at PSCP@hq.dhs.gov. The initial submission of the DHS Form 9014[1] to the PSCP Administrator does not require Social Security number (SSN), date of birth, or place of birth. Applicant name, contact information, job title, and justification are logged into a database maintained by the PSCP Administrator prior to being submitted for approval. The database resides on a restricted shared drive and is only accessible by the IP Security Office. No sensitive PII is maintained within this database. The IP Security Office is in the process of moving all information stored on the database to a DHS SharePoint page that will maintain all PII collected by PSCP from DHS Form 9014. Only the members of the IP Security Office, including the PSCP Administrator, supporting the PSCP will have access to the PSCP SharePoint site. If the Assistant Secretary for IP or the Office of Cybersecurity and Communications (CS&C)[2] does not approve the nomination or requests further justification prior to processing, the request form is returned to the PSCP Administrator. The PSCP Administrator notifies the Nominator of the need for additional information and/or non-concurrence and rationale. The Nominator then informs the Subject.

If approved by the Assistant Secretary, DHS Form 9014 is sent to the IP Security Office for further processing and submission to the DHS Office of the Chief Security Officer (OCSO). The IP Security Office contacts the Subject to obtain his or her SSN, date of birth, and place of birth. This information is only available to the Security Specialist within the IP Security Office working on the program and is directly entered into and maintained in the Integrated Security Management System (ISMS),[3] which is "owned" by OCSO. This two-part process helps minimize the collection of sensitive PII for only those Subjects who meet the threshold and are sponsored by DHS.

Upon collection of this information in ISMS, the IP Security Office enters the Subject's information into the U.S. Office of Personnel Management's (OPM) secure portal for investigation processing, the electronic questionnaire for investigation process (e-QIP). Specifically, the IP Security Office enters the following data into e-QIP: name, date of birth, place of birth, SSN, and business email address. The Subject accesses e-QIP directly to complete and submit OPM's online

[1] DHS Form 9014 is used to justify why the individual requires a clearance.
[2] The approval and signature by the Assistant Secretary for CS&C is a new requirement since CS&C will use the updated DHS Form 9014 to nominate and approve security clearances for its private sector partners as well.
[3] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.

security questionnaire, Standard Form 86, *Questionnaire for National Security Positions*. Once the Subject completes the forms in e-QIP, the Subject must provide the IP Security Office with copies of the e-QIP signature pages. These signature pages are part of a package of DHS forms and standard security forms 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 IP Security Office instructs Subjects 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. DHS OCSO works with OPM and follows its processes and standard operating procedures (SOP) for investigations and adjudications. The investigation file is not shared with the IP Security Office. OCSO notifies the IP Security Office and the Subject of the decision to grant or deny the security clearance via email.

DHS Form 9014 requests the following information (*Note: (*) denotes a new data element requested on the updated DHS Form 9014*):

- Applicant's name;
- Type of Submission;
    - Company change;
    - Initial submission;
    - Periodic reinvestigation;
    - Reciprocity; and
    - Reinstatement.
- Company name;
- Company address;
- Program through which the form is being submitted;*
- Phone number;
- Email address;
- Critical infrastructure sector;
- Level of clearance requested;
- U.S. citizenship (yes/no);

- Clearance justification (to include: job title, responsibilities, association memberships, previous clearance information if applicable); and
- Signatures of the Nominator and Assistant Secretary for IP or for CS&C.*

If the application is approved, the IP Security Office requests the following information over the phone:[4]

- SSN;
- Date of birth; and
- Place of birth.

In rare circumstances in which it is not possible for the applicant to provide his or her SSN, date of birth, and place of birth, the IP Security Office also accepts this information in an encrypted or password-protected document attached to an email sent to PSCP@hq.dhs.gov. Upon entry into ISMS and e-QIP, the PSCP team immediately deletes the document and deletes the email.

Since the February 11, 2015, PIA Update, management of PSCP moved from IP/Sector Outreach and Programs Division (SOPD) to the IP Security Office located in the IP Office of the Assistant Secretary's Office of Administration. In addition, PSCP now handles the private sector clearance application packages for programs across NPPD, specifically within IP and CS&C. These private sector partners for whom PSCP processes clearance application packages are subject matter experts within specific industries and have specialized knowledge not available within DHS. IP and CS&C programs sponsor clearances for these entities and individuals who are not employed by or contracted with the U.S. Government (the traditional means of obtaining a clearance) and must have clearances.

CS&C program managers whose programs offer clearances to private sector partners may now serve as nominators for a private sector partner's clearance. For all application requests from CS&C nominators, the signature of the Assistant Secretary for CS&C must now be obtained along with the CS&C Assistant Secretary's concurrence for the nomination. DHS Form 9014 is being updated to include nominators from CS&C and to include signatures by the Assistant Secretary for CS&C on those application requests from CS&C. Inclusion of CS&C nominations does not otherwise change the process[5] PSCP uses for application package management.

[4] Note that this information is not collected within DHS Form 9014. The IP Security Office submits this information directly into ISMS and into e-QIP to initiate the clearance process.
[5] For a thorough discussion of the PSCP Clearance Process, *see* DHS/NPPD/PIA-020(a) Private Sector Clearance Program for Critical Infrastructure, *available at* www.dhs.gov/privacy.

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

In the February 11, 2015, PSCP PIA Update,[6] the PSCP indicated that it would utilize a HSIN-CI website specific to PSCP as a security clearance management tool, which would maintain information received by PSCP for PSCP clearance holders and PSCP nominees. While IP took steps to implement the use of the website, the PSCP determined that it would continue to maintain the clearance management information it receives for PSCP clearance holders and PSCP clearance nominees in a password-protected folder housed in an IP/PSCP shared drive folder with access to the folder restricted so that only PSCP team members can access it. In addition, as of the development of this PIA update, PSCP is transitioning data into a SharePoint site to which only the PSCP team has access.

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

DHS Form 9014, *Private Sector Clearance Request Form*, was recently updated and is currently going through the Paperwork Reduction Act (PRA) process. The OMB Control Number is 1670-0013.

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 as its role increases within NPPD. For example, to help PSCP determine for which IP or CS&C program DHS Form 9014 is being submitted, the form now requests the program under which the application is being submitted. This will help the nominators and the Assistant Secretaries for IP and CS&C make their approval determinations.

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 mitigated by the fact that the new data fields on the updated DHS Form 9014 do not request PII from PSCP Nominees.

Uses of the Information

The HSIN-CI/PSCP site discussed in the February 11, 2015, PIA Update was never implemented. Thus, the risks and mitigations related to the Uses of Information in the February

[6] *See* DHS/NPPD/PIA-020(a) Private Sector Clearance Program for Critical Infrastructure, *available at* www.dhs.gov/privacy.

11, 2015, PIA Update do not apply. Therefore, there is no change from the November 11, 2011, PIA.

Notice

No change from the February 2015 PIA Update.

Data Retention by the project

No change from the February 2015 PIA Update.

Information Sharing

The HSIN-CI/PSCP site discussed in the February 11, 2015, PIA Update was never implemented. Thus, the risks and mitigations related to the Information Sharing in the February 11, 2015, PIA Update do not apply. Therefore, there is no change from the November 11, 2011, PIA.

Redress

No change from the February 2015 PIA Update.

Auditing and Accountability

No change from the February 2015 PIA Update.

Responsible Official

Cynthia Briscoe
Branch Chief, Security Office
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.

_____

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.