Privacy Impact Assessment

for the

State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure

DHS Reference No. DHS/CISA/PIA-020(c)

August 28, 2023

Homeland Security

Abstract

The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) is updating the Private Sector Clearance Program for Critical Infrastructure's (PSCP) Privacy Impact Assessment (PIA) to account for the organizational changes that have taken place in the administration of the program at CISA. This update outlines changes to the program clearance process and to DHS Form 9014, *State, Local, Tribal and Private Sector Clearance Request Form,* since the publication of the Privacy Impact Assessment Update in April 2018.

Overview

Protecting critical infrastructure security and resilience requires ongoing cooperation between government and private industry. While most information DHS shares with the private sector is at the unclassified level, some information may be classified, requiring a federal security clearance. Formerly known as the Private Sector Clearance Program for Critical Infrastructure, the renamed State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure 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. The scope will also be expanded to include State, Local, and Tribal applicants who require appropriate security clearances to access information relevant to the protection, security, and resilience of critical infrastructure assets in their jurisdictions. With security clearances, these owners, operators, and representatives can collaborate and crosstalk with federal offices and can access classified information to make more informed decisions. The State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure facilitates security clearance application processing for State, Local, Tribal, and private sector partners and is now administered by the CISA Office of the Chief Security Officer (OCSO).

Reason for the PIA Update

This Privacy Impact Assessment Update addresses changes that the CISA Office of the Chief Security Officer has made to the program since publication of the April 2018 Privacy Impact Assessment Update, including:

- The Private Sector Clearance Program for Critical Infrastructure that was previously under the purview of the DHS National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection is now the State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure and is under the purview of the CISA Office of the Chief Security Officer.

- The scope of the clearance program (and use of DHS Form 9014) now includes not only individuals from the private sector, but also State, Local, and Tribal applicants/nominees.
- The role of the CISA Office of the Chief Security Officer Personnel Security Specialist in the clearance process has expanded, replacing the State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure Administrator as the position responsible for data entry into the Integrated Security Management System (ISMS)[1] and collection of required documentation for higher level review by the Office of the Chief Security Officer prior to clearance approval.
- The clearance process within the CISA Office of the Chief Security Officer has been consolidated, eliminating submission to, and processing by, the DHS Office of the Chief Security Officer.
- The submission package of physical documents—including e-QIP signature pages, DHS forms, and standard security forms submitted before the investigation process begins—that were retained by the CISA Office of the Chief Security Officer has been eliminated. Only electronic packages of forms and fingerprints, including DHS Form 9014, are retained and submitted to a higher-level reviewer within the CISA Office of the Chief Security Officer for processing.
- Specific data fields related to the collection of information through DHS Form 9014, now called the *State, Local, Tribal and Private Sector Clearance Request Form*, have changed:
    - Applicant/nominee's personal email address is now included;
    - There are additional drop-down options for the type of submission and critical infrastructure sectors;
    - Applicant Signature fields are eliminated; and
    - The "Do Not Complete Below this Line" section of the form which included fields for the applicant's Social Security Number (SSN), Date of Birth, Place of Birth, and Mailing Address are eliminated.
- Now includes reference to the sunsetting of the OPM Electronic Questionnaire for Investigation Processing (e-QIP), which is scheduled to take place in October 2023 and be replaced by National Background Investigation Services (NBIS) eApplication (eAPP) as the system for initiating investigations. The use of the new eAPP system will not differ

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED SECURITY MANAGEMENT SYSTEM (ISMS), DHS/ALL/PIA-038, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

from how State, Local, Tribal, and Private Sector partners currently use e-QIP. Both e-QIP and e-APP are referenced below in the State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure Process Update.

Administrative/Organizational Update

Since the April 2018 Privacy Impact Assessment Update, the management of the State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure moved from Infrastructure Protection/Sector Outreach and Programs Division in the (former) National Protection and Programs Directorate to the CISA Office of the Chief Security Officer. While there are no changes to the purpose of the program, the scope has expanded to include State, Local, and Tribal applicants who require appropriate security clearances to access information regarding the protection, security, and resilience of critical infrastructure assets in their jurisdictions. The State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure, like the Private Sector Clearance Program in the National Protection and Programs Directorate, continues to sponsor and process security clearances for individuals who are not employed by or contracted with the U.S. Government (the traditional means of obtaining a clearance) yet must maintain a security clearance.

State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure Process Update

Within the CISA Office of the Chief Security Officer, a central State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure Administrator receives clearance requests and processes applications. Sector Risk Management Agencies, Regional Sector Outreach Coordinators, Protective Security Advisors, CISA/Infrastructure Security Division Sector Liaisons, CISA Central, and other federal officials designated by CISA may serve as nominators of security clearance requests. Nominators identify individuals who need a DHS-sponsored security clearance. The nominated individual must have a CISA-related mission and meet the requirements and criteria as outlined in the policies that govern the State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure before submission through the CISA Action Task Tracking (CATT)[2] system. The Nominator and the individual complete DHS Form 9014. After approval by the appropriate CISA divisional senior level official, the completed form is forwarded to the Administrator via the CISA Action Task Tracking system.

The initial submission of DHS Form 9014 to the Administrator does not require the individual's Social Security number, date of birth, place of birth, or home mailing address.

[2] The CISA Action Task Tracking system is an administrative tasking system used to route requests and approvals to appropriate offices. For more information on these types of systems at the Department, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR DHS CORRESPONDENCE AND INQUIRIES TRACKING TOOLS, DHS/ALL/PIA-007, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

Applicant name, contact information, job title, and justification are logged into a SharePoint database maintained by the Administrator before submission to the CISA Office of the Chief Security Officer Personnel Security Specialists to commence the security clearance process. Access to the SharePoint database is provisioned on a need-to-know basis. If any discrepancies are identified, the Administrator will notify the nominating CISA Division Executive Secretary Office to make any needed edits or corrections.

If approved by the CISA senior level official,[3] the Administrator electronically sends the DHS Form 9014 to the CISA Office of the Chief Security Officer for further processing. The signed DHS Form 9014 is then saved on a restricted shared drive folder, only accessible by the CISA Office of the Chief Security Officer. The CISA Office of the Chief Security Officer contacts the individual via e-mail to obtain their Social Security number, date of birth, and place of birth. This information is only available to the CISA Office of the Chief Security Officer Personnel Security Specialist who directly enters and maintains it in the Integrated Security Management System. The email responses containing the sensitive personally identifiable information are requested by the CISA Office of the Chief Security Officer to be password protected or encrypted and must be saved in that manner in the restricted share drive folders.

Upon collection of the required information in the Integrated Security Management System, the Personnel Security Specialist enters the individual's information into OPM's secure portal, e-QIP or, as of October 2023, its replacement system the National Background Investigation Service's eAPP. Specifically, the Personnel Security Specialist enters the following data into e-QIP/eAPP: applicant name, date of birth, place of birth, Social Security number, and business email address. The applicant may then access e-QIP/eAPP directly to complete and submit OPM's online security questionnaire, Standard Form 86 (SF-86), *Questionnaire for National Security Positions*. Once the individual completes the forms in e-QIP/eAPP, they must provide the Personnel Security Specialist with electronic copies of the e-QIP/eAPP 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 electronic fingerprints and a DHS Form 11000-9, *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act*.

The Personnel Security Specialist sends the complete, electronic package of forms and fingerprints, including DHS Form 9014, to a higher-level reviewer within the CISA Office of the Chief Security Officer for processing. The CISA Office of the Chief Security Officer notifies the Nominee of the decision to grant or deny the security clearance via email.

[3] CISA Executive Assistant Director(s)/Deputy Executive Assistant Director(s), Assistant Director(s)/Deputy Assistant Director(s), Regional Director(s), CXO(s)/Deputy CXO(s) of the sponsoring Division/Office are designated as Final Approvers for nominations.

Privacy Impact Analysis

Authorities and Other Requirements

DHS Form 9014, *State, Local, Tribal and 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 State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure, the CISA Office of the Chief Security Officer is expanding the categories of information collected. DHS Form 9014 is being updated to request additional data elements from State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure Nominees as well as Nominator information described above. The update to the form is in conjunction with the expansion of the clearance program to now include nominations of State, Local, and Tribal applicants. Applicants now have the opportunity to provide more specificity as it relates to the sectors of critical infrastructure in which they would require clearance and the type of clearance needed, as well as the ability to provide the best contact information possible for correspondence with CISA throughout the clearance process. This helps CISA ensure adequate representation of all 16 Critical Infrastructure sectors and CISA-led councils to include state, local, tribal, and elections officials.

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

- Applicant's name;
- Company Name;
- Company Address;
- Phone Number;
- Email Address (Business and Personal*);
- Clearance Level Needed;
- Job Position;
- Type of Submission:
    - *Company Change;*
    - *Initial Submission;*
    - *Periodic Reinvestigation;*

  - *Reciprocity;*
  - *Reinstatement;*
  - *Upgrade;* or*
  - *Downgrade.**

- Program Type through which the form is being submitted:
  - *Classified Critical Infrastructure Protection Program (CCIPP);*
  - *Cyber Information Sharing and Collaboration Agreement (CISCA);*
  - *Cooperative Research and Development Agreement (CRADA);*
  - *National Security Telecommunications Advisory Committee (NSTAC);*
  - *Private Sector; or*
  - *State, Local, and Tribal.*
- Critical Infrastructure Sector:
  - *Chemical;**
  - *Commercial Facilities – Entertainment and Media;**
  - *Commercial Facilities – Gaming;**
  - *Commercial Facilities – Lodging;**
  - *Commercial Facilities – Outdoor Events;**
  - *Commercial Facilities – Public Assembly;**
  - *Commercial Facilities – Real Estate;**
  - *Commercial Facilities – Retail;**
  - *Commercial Facilities – Sports Leagues;**
  - *Communications;**
  - *Dams;**
  - *Defense Industrial Base;**
  - *Emergency Services;**
  - *Energy – Electric;**
  - *Energy - Oil and Gas;**
  - *Faith Based Outreach;**

- *Financial Services;**
- *Food and Agriculture;**
- *Government Facilities – Education Facilities;**
- *Government Facilities – Election Infrastructure;**
- *Government Facilities – National Monuments/Icons;**
- *Healthcare and Public Health;**
- *Information Technology;**
- *National Infrastructure Advisory Council (NIAC);**
- *Non-Profit Organization;**
- *National Security Telecommunications Advisory Committee;**
- *Nuclear Reactors, Material and Waste;**
- *Transportation Systems – Aviation;**
- *Transportation Systems – Hwy Motor Carrier;**
- *Transportation Systems – Maritime;**
- *Transportation Systems Trans – Pipeline;**
- *Transportation Systems – Postal and Shipping;**
- *Transportation Systems – Public Transit;* or*
- *Transportation Systems – Rail.**

- U.S. Citizenship (Yes/No); and
- Justification of Need to Access Classified Information.
- Nomination Information:
  - Nominator Name;
    - Position;
      - CISA Sector Risk Management Agency (SRMA);
      - Non-CISA Sector Risk Management Agency (SRMA);
      - Protective Security Advisor (PSA);
      - Regional Sector Outreach Coordinator (RSOC);
      - Sector Liaison;

- Chief Chemical Security Inspector;
- Supervisor Chemical Security Inspector;
- Chemical Inspector;
- Cybersecurity Inspector; or
- Other.

- Signature; and
- Date.

- Signature Authority;
  - Position;
    - Regional Director;
    - Deputy Regional Director;
    - Executive Assistant Director;
    - Assistant Director;
    - Deputy Executive Assistant Director/Assistant Director; or
    - Other.
  - Signature; and
  - Date.

If accepted by a CISA senior level official, the form is sent to the CISA Office of the Chief Security Officer for further processing. A Personnel Security Specialist will request the following sensitive personally identifiable information separately via password protected or encrypted email to continue the clearance process:

- Date of Birth;
- Place of Birth;
- Social Security Number; and
- Home Mailing Address.

Privacy Risk: There is a privacy risk that DHS may collect more information than is necessary because of the additional data elements in the updated DHS Form 9014.

Mitigation: This risk is mitigated. The additional data field in the DHS Form 9014 that collects the personal email address of the State, Local, Tribal and Private Sector Clearance

Program for Critical Infrastructure Nominee has been added to the form to better ensure correspondence between State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure program personnel and the Nominee during the clearance process. The process itself is no different if initiated by personal email, and any privacy risk is further mitigated by the two-step collection process, which allows sensitive personally identifiable information to be collected only from those nominees who are approved for a security clearance, after the initial approval of the DHS Form 9014. The form has been further updated to remove data collections that are unnecessary at that point in the process.

Uses of the Information

No change from the original November 2011 Privacy Impact Assessment.

Notice

No change from the April 2018 Privacy Impact Assessment Update.

Data Retention by the Project

No change from the April 2018 Privacy Impact Assessment Update.

Information Sharing

No change from the original November 2011 Privacy Impact Assessment.

Redress

No change from the April 2018 Privacy Impact Assessment Update.

Auditing and Accountability

No change from the April 2018 Privacy Impact Assessment Update.

Contact Official

Eric Novotny
Associate Chief, Personnel Security Division
Office of the Chief Security Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
CISAOCSPSD@cisa.dhs.gov

Responsible Official

Kerry Stewart
Chief Security Officer

Office of the Chief Security Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
Department of Homeland Security