Privacy Impact Assessment

for the

Credibility Assessment and Polygraph Services (CAPS)

DHS Reference No. DHS/CBP/PIA-064

July 16, 2020

Homeland Security

Abstract

The U.S. Customs and Border Protection (CBP), Office of Professional Responsibility (OPR), Credibility Assessment Division (CAD) administers polygraph examinations as part of the hiring process for CBP Officers and Agents to assist in determining suitability for employment, and in support of internal and counterintelligence investigations. CAD uses the Credibility Assessment and Polygraph Services (CAPS) system in support of its polygraph examination program. CBP is conducting this Privacy Impact Assessment (PIA) on CAPS because the system ingests, uses, and maintains personally identifiable information (PII) from members of the public who are candidates for law enforcement positions with CBP or a partner agency.

Overview

CBP conducts background investigations on applicants for employment to ensure that candidates meet the suitability or fitness requirements for employment as a federal employee or contractor, eligibility for access to federal facilities, automated systems, or classified information, and/or eligibility for issuance of a CBP credential. As part of the background investigation process, CBP is mandated by the Anti-Border Corruption Act of 2010[1] to conduct polygraph examinations on all applicants for its law enforcement positions. With approximately 150 authorized OPR analysts, CAD is responsible for the administration of polygraph examinations. In addition to conducting polygraph examinations on candidates for law enforcement positions, CAD also conducts examinations on CBP employees who are subject to counterintelligence[2] or other investigations (e.g., misconduct),[3] and applicants or employees of other U.S. Department of Homeland Security (DHS) Components or other federal departments and agencies with whom CBP has reciprocal agreements.

CAD uses the CAPS system, a web-based application created by CBP, to support its polygraph examination process. CAPS streamlines the scheduling, execution, and archiving of the polygraph process. CAPS enhances data quality, validation, and reporting of statistics (aggregated information) related to polygraph assessments. CAPS uses information retrieved from other CBP human resources and OPR systems to build a record for the subject in preparation for the polygraph exam. CAPS stores the polygraph examination records, results, and reports. CAPS also contains a correspondence section to maintain complaints or formal requests for information, such as Equal Employment Opportunity (EEO) actions, Congressional letters, Freedom of Information Act (FOIA) requests, and other requests related to a subject's polygraph test.

---

[1] 6 U.S.C. § 221.

[2] Counterintelligence examinations are geared towards the CBP Office of Intelligence positions and screen for issues associated with intelligence and national security information.

[3] Current employees are not subjected to a periodic reinvestigation polygraph examination. If a current employee is receiving a polygraph examination, it is because they are part of an ongoing investigation of alleged misconduct.

Hiring and Suitability

The polygraph process begins after the CBP OPR Personnel Security Division (PSD) receives the completed Office of Personnel Management (OPM) standard government forms noted in Section 1.5 from an individual who has received a tentative selection offer of employment from CBP.[4] Candidates can access, complete, and submit the standard government forms for employment and eligibility through the OPM Electronic Questionnaires for Investigations Processing (e-QIP) system.[5] CBP's Human Resources Business Engine (HRBE)[6] system initiates the background investigation process by sending a link to the individual to complete the OPM e-QIP form online. OPM electronically sends the completed e-QIP form to HRBE and the information is electronically sent from HRBE to the CBP Cornerstone System.[7] HRBE exchanges information with the DHS Integrated Security Management System (ISMS) [8] and Cornerstone nightly to update case information in both systems.

PSD personnel manually enters the status for the background information into ISMS and assigns the case to CAD. ISMS automatically transfers the status to HRBE to confirm that the background investigation is initiated. PSD conducts the pre-polygraph vetting checks and records any information relevant to the background of the applicant and to the polygraph examination (such as derogatory information) in ISMS. Once completed, OPR PSD notifies CBP Human Resources Management (HRM) and CAD that the subject is ready for the polygraph examination.

CBP implemented a system interface between CAPS and Cornerstone in order to retrieve information regarding the status of individuals requiring polygraph examinations. CAPS imports the list of applicants, and automatically reviews applications against business rules to ensure all required actions are completed prior to record creation in CAPS. The imported applicants are automatically put in an unassigned queue in CAPS, at which point a CAD analyst conducts a manual upload of each applicant's e-QIP forms, and any other relevant information, from ISMS into CAPS. The CAD analyst then transmits a scheduling request to the applicant, either automatically through the CAPS scheduling system or via email.

CAD uses CAPS to store all relevant documentation related to the polygraph examination

[4] A tentative offer of employment is preliminary when it is pending a successful background investigation and suitability determination.
[5] OPM manages e-QIP, a secure website that is designed to automate the common security questionnaires used to process federal background investigations. CBP applicants will access e-QIP through the OPM website, and upon completion, OPM sends applicant information to CBP's HRBE. For additional information, please see http://www.opm.gov/privacy/PIAs/eQIP.pdf.
[6] *See* DHS/CBP/PIA-032 Human Resources Business Engine, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[7] DHS/CBP/PIA-038 Cornerstone, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[8] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

but does not use the system during the administration of the exam itself. After the polygraph examination is completed, CAD collects documentation from the individual and manually uploads the information into CAPS. This documentation may include:

- medical liability forms;
- consent forms;
- confidentiality forms; and
- any additional forms for individuals returning for additional testing.

If the applicant provides a written statement (such as an admission), that form is also uploaded into CAPS.

In addition, the polygraph examiner consolidates the polygraph results and manually uploads the information to CAPS. These results may include:

- the polygraph charts;
- audio recordings;
- written test questions; and
- test data analysis or scoring sheets.

The examiner may also upload any other information or documentation that may be relevant to the exam (such as a cancelation request, any updated information submitted by the subject).

Once the examiner uploads the relevant documentation into the system and completes all the required fields, he or she submits the package electronically within CAPS for the CBP quality control (QC) team's final review. The QC analyst downloads the relevant files from CAPS and reviews the examination charts and audio recordings in polygraph software, and manually enters his or her final review into the QC section of CAPS. CAPS contains drop-down menus with results that reflect the QC scoring, including the final results (e.g., inconclusive, no opinion, no significant response). Once the QC process is complete, if the QC analyst concurs with the assessment, then the examination process is concluded once all testing has been completed. If the QC analyst identifies issues, additional testing may be required, and the assessment is placed back in the examiner queue, at which point the examiner's process starts from the beginning with scheduling the exam. If no additional testing is required, then CAPS generates the polygraph report.

The final polygraph assessment report is an auto-populated document generated based on biographic information received from ISMS, HRBE, and the polygraph assessment. The polygraph assessment report provides an outline of what occurred during the polygraph requirement phase, how many times a polygraph test(s) was administered to the individual, if there were any admission(s) made by the applicant, and the final polygraph result (i.e., Pass/Fail). The report

remains available in CAPS, but a copy of the assessment report is uploaded to ISMS as part of the adjudication record. OPR PSD uses this report, along with results of the background investigation, to make a final suitability determination. While CAD personnel conduct the polygraph examinations, OPR PSD is responsible for all suitability adjudications.

Other Agency, Counterintelligence, and Issue-specific Investigations

The process for conducting polygraph examinations for other federal department and agency personnel, counterintelligence investigations, and other issue-specific investigations mirrors the process outlined above, and the polygraph materials collected in CAPS are the same. The primary difference is the source of the information:

- For other federal department and agency personnel (e.g., any subject who has not applied for employment with CBP but has been referred to CBP by their home agency, which may be a DHS Component or another federal agency), the bulk of the information is sourced from the subject directly, although information may also be provided by a case agent, current supervisor, or Chief Security Officer or designee.
- For counterintelligence examinations, which occur when a subject requires higher level security clearance for a position, the information is provided by the subject directly or from a case agent, current supervisor, or Chief Security Officer or designee.
- For examinations pursuant to misconduct or other specific-issue investigations, which occur when polygraph assistance is requested by CBP OPR Investigative Operations Division (IOD) or other agency investigative divisions, the information is sourced by the investigative office or agency.

Correspondence Records

CAPS contains a correspondence section for the archiving and tracking of formal requests for information deemed relevant to the administration of polygraph examinations and to track any actions taken by CAD in response to those requests. The correspondence includes complaints or formal requests, such as EEO actions, Congressional letters, FOIA requests, and other requests related to any polygraph test administered. All such correspondence pertaining to the polygraph program is maintained in its own module within CAPS. CAD employees assigned in the system as an Administrator, Assistant Special Agent in Charge (ASAIC), Queue Manager (QM), or QC, have access to this module and manually enter the data required to track these inquiries.

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?

CBP conducts polygraph examinations pursuant to the following authorities:

- Public Law 111-376, Anti-Border Corruption Act of 2010;
- Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (Dec. 17, 2004), mandating federal agencies ensure the appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and reciprocity of determining eligibility for access to classified national security information;
- 6 U.S. Code (U.S.C.) § 221, requirements with respect to administering polygraph examinations to all applicants for law enforcement positions with CBP;
- Security Executive Agent Directives (SEAD) 1, 2, and 7, Office of the Director of National Intelligence (pursuant to Executive Order 13741: Amending Executive Order (E.O.) 13467, to Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters);
- 18 U.S.C. § 1001, Crimes and Criminal Procedure, Statements or entries generally;
- Public Law 82-298, Authority for Conducting Certain Personnel Investigations;
- Title 5, Code of Federal Regulations (C.F.R.) Part 731, Suitability;
- Title 5, C.F.R. Part 732, National Security Positions;
- Title 5, C.F.R. Part 736, Personnel Investigations;
- Title 5, C.F.R. Part 1400, Designation of National Security Positions;
- Title 32, C.F.R. Part 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information;
- E.O. 10450 (Apr. 27, 1953) – Security Requirements for Government Employment;
- E.O. 12968 (August 2, 1995) – Access to Classified Information;
- E.O. 10865 (February 20, 1960) – Safeguarding Classified Information within Industry;
- E.O. 12356 (April 2, 1982) – National Security Information;
- E.O. 13467 (July 2, 2008) – Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;

- DHS Directive 121-01-02, Chief Security Officer (May 21, 2018) – assigns authority for DHS security programs to the DHS Office of the Chief Security Officer (OCSO), which is directed to oversee DHS personnel security policies, programs, and standards; deliver security training and education to DHS; and provide personnel security support to DHS components. The directive sets procedural guidelines for DHS's security functional integration, including standardization of security policies and appropriate procedures and continued consolidation and integration of systems[9] supporting DHS's security functions; and
- DHS Delegation 12000 (June 5, 2012), Delegation for Security Operations within the Department of Homeland Security.

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

Data in CAPS is covered by the following System of Records Notices (SORN):

- DHS/ALL-023 Personnel Security Management System of Records[10] describes CBP's collection and maintenance of information related to personnel security actions and the resulting determinations. It covers any individual seeking access to DHS-owned facilities, DHS information technology systems, and national security information.
- DHS/ALL-004 General Information Technology Access Account Records System[11] describes CBP's collection and maintenance of PII for the purpose of providing authorized individuals access to DHS information technology (IT) resources and to track the use of those IT resources. It covers those individuals who are authorized to access DHS IT resources, such as employees, contractors, grantees, private enterprises, and any lawfully designated representative, in furtherance of the DHS mission.

[9] ISMS is owned and operated by the DHS OCSO. ISMS stores background investigation information that all component personnel security divisions use as part of their adjudicative processes. However, most components do not require a polygraph for their employees. Therefore, while CBP uses ISMS for biographic information submitted as part of the suitability process, ISMS does not have reporting and storage capability robust enough to conduct and maintain the CBP polygraph reports, results, and correspondence.
[10] *See* DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns. This SORN is currently in the process of being updated.
[11] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2013), *available at* https://www.dhs.gov/system-records-notices-sorns.

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

CBP granted CAPS an Authority to Operate (ATO) in August 2017, consistent with DHS Sensitive Systems Policy Directive 4300A.[12] This ATO will be renewed in advance of its expiration date in August 2020.

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

In general, CAPS is covered by a legacy U.S. Customs Service NARA-approved Records Disposition Authority Job Number N1-36-92-1 certified on November 9, 1993, which pertains to Personnel Security Clearance Files. Various types of records are created and maintained during the course of the hiring process to assist with the tracking an employee who applies for federal civil service. The types of records that are covered by the SORNs listed in Section 1.2 include: suitability investigations; general testing; standing inventory of jobs; employee eligibility; case examining; and examinations under litigation. Each of these record types has its own NARA-approved retention and disposal schedule. OPR is working with the CBP Records Officer to formalize a retention schedule for CAPS. See Section 5.0 for additional information regarding records retention.

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.

CAPS maintains information housed in other CBP systems and collected originally by OPM via e-QIP using Standard Forms (SF): SF-85, SF-85P, or SF-86,[13] and these forms are therefore covered by the PRA. The OMB control numbers for this information are:

- Standard Form 85, Questionnaire for Non-Sensitive Positions, OMB No. 3206-0005.
- Standard Form 85P, Questionnaire for Public Trust Positions, OMB No. 3206-0191.
- Standard Form 86, Questionnaire for National Security Positions, OMB No. 3206-0005.

The PRA does not apply to other collections related to the polygraph examination.

[12] *See* DHS Sensitive Systems Policy Directive 4300A (July 27, 2017), *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.
[13] OPM Standard Forms (SF) are available at: https://www.opm.gov/forms/standard-forms/.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information entered into CAPS for individuals undergoing suitability assessment, regardless of the classification of the subject (i.e., federal employee, contractor, or applicant), originates from HRBE, ISMS, or Cornerstone. For individuals subject to an internal agency investigation or counterintelligence exam, information may come from the investigator and/or the subject themselves.

CAPS contains the following information from HRBE:

- Social Security number[14] – collected as unique identifier prior to creation of a HASH ID.[15] A HASH ID is not issued if the applicant does not become a CBP employee;
- First Name;
- Last Name;
- Date of Birth;
- Place of Birth;
- City of Residence – used to determine to what office the case will be assigned;
- State of Residence – used to determine to what region the case will be assigned;
- Phone Number – used to contact examinee; and
- Email Address – used to contact examinee.

CAPS also maintains certain information from Cornerstone including:

- Position Handle;
- Date the OPR PSD case was opened;
- Date that forms were received by OPR PSD; and
- Case Work Status for the Pre-Appointment Case.

[14] CBP requires the use of the SSN during the background investigation and polygraph process due to the continued reliance on SSN by OPM as a candidate identifier, and because many applicants for employment with CBP have similar names and dates of birth. Since not all applicants are selected for employment, and because CBP must link the suitability action back to the candidate selection action with OPM, it is not possible for CBP to generate a different unique identifier for use as part of this process.

[15] HASH ID is a unique CBP ID given to CBP employees and contractors to gain access to CBP systems. CBP does not issue HASH IDs to applicants who do not pass the polygraph.

CAPS maintains the following information from ISMS:

- Uploaded e-QIP information (SF-86).

CAPS maintains various uploaded documents related to the polygraph examination, including:

- CBP Form 329, Polygraph examination consent;
- CBP Form 330, Applicant Confidentiality Agreement for CBP Polygraph Exams;
- CBP Form 331, Applicant Release of Liability Form for additional testing;
- CBP Form 332, Purposeful Non-Cooperation Notice;[16]
- Any statements from the applicant, including admission statements;
- Medical liability form;
- Notes, correspondence, or other documentation deemed relevant by the polygraph examiner;
- Polygraph examination results, including charts, audio recordings of the examination, written test questions, and test data evaluation/scoring sheet; and
- Relevant case notes or investigatory materials related to examinations for internal affairs and counterintelligence investigations.

CAPS also maintains information related to Congressional inquiries, complaints, FOIA requests, and other official correspondence related to polygraph examinations. This information may include:

- Requestor name and contact information;
- Relevant documentation related to the response; and
- Results of any reviews completed on correspondence.

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

The majority of the information entered into CAPS is originally collected from the subject and is populated in CAPS from other CBP systems (listed below). Most of this information is originally obtained from the standard forms through the OPM e-QIP system.

CBP and DHS systems that provide information to CAPS include:

[16] The Purposeful Non-Cooperation Notice serves as a reminder to applicants that the successful completion of the pre-employment polygraph examination is a requirement to be hired in a Federal law enforcement position with CBP and acknowledgement to understand the potential implication of non-cooperation.

- HRBE: CBP developed a secure, access-controlled web service connections between HRBE and Cornerstone, and the data is subsequently transmitted through Cornerstone to ISMS. This web service allows for exchange of biographical data, and provides CAD with the required information to contact, schedule, and conduct polygraph assessments.
- Cornerstone: In order to retrieve certain information, CBP developed a secure, access-controlled web service connection to exchange information with three web-based systems. Cornerstone sends the applicant's information, position information for the vacancy, and investigation status information to ISMS. CAPS and Cornerstone facilitate the exchange of information regarding the status of certain applicants requiring polygraph examinations.
- ISMS: authorized CAD analysts access ISMS to create a polygraph record and retrieve the e-QIP form, and Cornerstone automatically retrieves and uploads the e-QIP form into CAPS to conduct their analysis. At the completion of the polygraph exam, CAD analysts update the polygraph record in ISMS and upload the final polygraph report and results.

The remainder of the information is entered into the system by the polygraph examiner or other authorized OPR employee.

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

In general, CAPS does not maintain any commercially or publicly available data. However, CBP examiners may research information found on the Internet to verify details provided by an applicant or employee to PSD during the background investigation.

2.4 Discuss how accuracy of the data is ensured.

PII maintained in CAPS is sourced from other CBP systems. Individuals submitting information into these systems (including the subject of the investigation completing the required forms) are provided an opportunity to review the information and must certify its accuracy prior to submission. CAD analysts review information for duplication (i.e., previous applications and polygraph examination results for employment by the same individuals) to resolve identity discrepancies and ensure that records in the system pertain to the correct individual. Records deemed to be duplicate are flagged for further analysis to verify if previous results are still valid.[17]

In addition, CAD personnel verify all biographic information with subjects during the polygraph examination and make any necessary changes in CAPS in the event of an error. The polygraph examinations administered by CBP has been researched, approved, and inspected for

[17] Polygraph examination results are valid for two years and maintained in the respective system(s) consistent with personnel security records retention schedules and SORNs.

use by the National Center for Credibility Assessment (NCCA). NCCA maintains federal oversight of all executive branch agencies who administer polygraphs in support of personnel security vetting for initial or continued eligibility for access to classified information or eligibility to hold a national sensitive position, as stated in the SEAD 2. SEAD 2 directs all these executive level agencies to submit to NCCA biennial inspections.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that CAPS may retain more information than is necessary to administer the polygraph and assist in determining the individual's suitability for employment with CBP.

Mitigation: This risk cannot be mitigated. CBP must collect a wide-range of information in order to conduct a thorough assessment to ensure applicants for law enforcement positions with CBP are reliable, trustworthy, and of good conduct and character. Doing so requires a comprehensive background investigation that necessarily collects a large amount of information about an individual. The information accessed for the polygraph assessment, which is similarly expansive, is required in order to validate or further investigate the findings of the background investigation.

Privacy Risk: There is a risk that CBP may rely on inaccurate results from a polygraph.

Mitigation: This risk is mitigated. There are inherent accuracy risks associated with credibility assessments. However, CBP has taken considerable steps to mitigate these risks. CBP provides an opportunity for individuals to discuss the results of the polygraph examination and based on that information, CAD may complete additional testing. All CBP credibility assessments are accredited and reviewed by the NCCA on a biennial basis. In addition, CAD personnel administer the polygraph exam, but suitability determinations are made by the OPR PSD division to ensure lack of bias or inappropriate input from the credibility assessors. OPR PSD investigators also use the polygraph results as a means to conduct further investigation and verification into an applicant's background and trustworthiness; the polygraph results themselves are not dispositive of a finding of unsuitability.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP uses CAPS to facilitate polygraph examinations to assess suitability for applicants for employment with CBP. CAPS serves as a workbench to streamline the process of polygraph assessments for CBP applicants and issue-specific investigations (e.g., misconduct). CAD also collaborates with other federal and international law enforcement entities in completing the

analyses of polygraph examinations of their subjects. CAPS enhances data quality, validation, and reporting of statistics (aggregated information) related to polygraph assessments. OPR/CAD employees use the information in CAPS to verify the individual being administered the polygraph is in fact the intended individual by checking the identity and comparing to the information listed. The biographical information and results of the polygraph examination are then populated into a final report that is uploaded into ISMS.

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. CBP uses CAPS data in support of the polygraph and credibility assessment processes. The information in CAPS is not subject to any analysis based on predictive pattern or anomalies.

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

No. Only CBP employees or CBP contracted personnel access CAPS. In the event that a polygraph examination uncovers a potential threat or other issue that requires further investigation, CAD may provide CAPS information to other divisions within CBP OPR. In such cases, the information is routed outside of CAPS, as other divisions do not have direct access to CAPS.

CBP may share information from CAPS as outlined in Section 5 below.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the sensitive information in CAPS will be used for a purpose other than internal affairs and personnel security activities.

Mitigation: This risk is mitigated. Access to CAPS is limited to a small group of authorized employees or vetted contracted personnel who have undergone a full background investigation and have been trained on the appropriate use of sensitive information. CAD only shares CAPS or polygraph information with individuals who have an established need-to-know for internal affairs and personnel security activities within the OPR IOD and Threat Mitigation Analysis Division, and other CBP Intelligence Offices, which is consistent with the original purpose of the polygraph examination.

When an examination is given to an applicant or employee of other DHS components or federal departments and agencies with whom CBP maintains a reciprocal agreement, CBP verifies the purpose of each individual request for information from the requesting entity. CBP manages information sharing procedures with other DHS components and partnering federal departments and agencies consistent with the routine uses described in the SORNs noted in Section 1.2.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CAPS receives much of its information from ISMS and HRBE. HRBE serves as the source system for information from e-QIP, USA Staffing, and other sources. The source systems maintain this information from individuals applying for employment or completing the required paperwork for security and suitability assessments. Whether the individuals provide this information via paper forms or electronically, they are provided with a collection notice required by the Privacy Act, 5 U.S.C. § 552a(e)(3). The Privacy Act Statement notifies the individual that the disclosure is considered voluntary and includes reasons for collecting the requested information, the consequences of failing to provide the requested information, explanations of how the information is used and with whom it is shared, and when and how information is deleted or disposed of. The collection, use, maintenance, and disclosure of information complies with the Privacy Act and the published SORNs cited in Section 1.2 above.

Before providing information in e-QIP, an individual confirms that he or she has been provided with and has read the Privacy Act Statement, agrees to participate in the suitability and clearance background investigation process (including credit checks and investigations which result in a Report of Investigation (ROI)), and submits to a name-based threat background check commensurate with the sensitivity of the position.

Prior to beginning the polygraph examination, the subject is required to review and sign a consent form, as well as a waiver and release of liability. These forms advise the subject of their rights with regard to the polygraph examination. In addition, the CBP Privacy Office is working with OPR to develop Privacy Act Statements for all of the relevant polygraph forms.

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

Individuals seeking employment with CBP provide their information on a voluntary basis and have an opportunity to consent, decline, or opt out at the time the information is collected. Prior to conducting the security and suitability assessments, the individual is requested to complete the CBP Forms 329, 330, and 331. Completing the forms is voluntary; however, individuals who choose not to submit the required information to CBP may be disqualified from employment. The polygraph examination is required by law for certain law enforcement positions with CBP and

individuals who opt out of the exam may not proceed further in the hiring process and will not be offered a position based on the failure to meet a condition of employment.

4.3 Privacy Impact Analysis: Related to Notice

There is no risk to notice. The information collected in CAPS originates with the subject of the examination, either through the pre-employment security forms, or through answers and other information provided by the individual during the application. Individuals seeking employment with other agencies who are referred to CBP for their polygraph examinations are aware that CBP collects and maintains this information on behalf of the requesting agency by virtue of the Privacy Act Statements on the forms and the release and waiver statements that are required prior to the examination.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

Consistent with legacy U.S. Customs Service schedules, as well as the retention schedule for personnel security records according to General Records Schedule (GRS) 5.6, Item 230, OPR intends to maintain information in CAPS for 25 years. OPR is working with the CBP Records Officer to formalize the retention schedule for CAPS.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CBP will retain information in CAPS for longer than is required.

Mitigation: This risk is partially mitigated. OPR is working with the CBP Records Office to formalize the records schedule for the information in CAPS. Until this occurs, CAPS will continue to safeguard the records in the system and will begin developing procedures to ensure that CAPS information is deleted from the system in accordance with GRS 5.6, Item 230, which allows CBP to destroy records 25 years after close of inquiry, but longer retention is authorized if required for business use.

Section 6.0 Information Sharing

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.

Information in the form of the Polygraph Report is only shared with other federal departments/agencies when the reciprocity of a polygraph examination analysis or report is requested and determined to be permissible, in addition to federal law enforcement cases and

investigative RFIs as noted above. Disclosures to federal law enforcement authorities may also be made if, during the course of an investigation, the discovery of a grievous criminal activity (e.g., child abuse, human trafficking) occurs. Any dissemination of information is logged for disclosure record keeping purposes, and all requests and disclosures are tracked in CAPS. There is no direct connection to any non-DHS systems. All information sharing occurs on a case-by-case basis when information is shared within DHS to components other than CBP, and when external departments/agencies requests (and if the sharing is deemed permissible) are made.

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

This information sharing is consistent with the purpose of the SORNs listed in Section 1.2, which is to ensure that individuals employed by CBP (or agencies it supports with its polygraph program) are suitable based on federal and agency standards. Sharing for the purposes listed in the SORNs is directly related to verifying an individual's initial and ongoing suitability.

6.3 Does the project place limitations on re-dissemination?

In the event that CBP shares information on its own applicants and employees with another party, it generally requires that the recipient not share the information with a third party without first requesting approval from CBP. This requirement is documented in the memoranda addressed to the recipient each time governing either the ad-hoc or bulk sharing of these records and any applicable dissemination rules.

External federal agencies may request background investigation information from CBP.[18] In such cases, the partner agency may share polygraph information with third parties as appropriate and consistent with their own authorities and any governing SORNs. CBP does not place limitations on onward sharing in such instances.

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

CAPS maintains a system log of all information shared with external sources. Disclosure records for information collected or passed through CAPS and subsequently disclosed from a record repository (e.g., ISMS) are maintained in accordance with disclosure requirements of that repository. Typically, OPR PSD processes all requests for background investigation information. In the event that CAD shares records from CAPS, the CAD staff uploads the request to the assessment or correspondence section in CAPS and completes a DHS Form 191 which is an

[18] *See* Executive Order 13488 – Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust (74 FR 4111), *available at* https://www.gpo.gov/fdsys/pkg/FR-2009-01-22/pdf/E9-1574.pdf.

accounting of a disclosure outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CBP will share information from CAPS in a manner inconsistent with the purpose of the original collection.

Mitigation: This risk is mitigated. CAPS users have security clearances and fulfill the required training for accessing sensitive information. This training includes notice of disciplinary action for those who mishandle PII and other sensitive information. CAPS logs all actions within the system associated with the user so that inappropriate use may be identified. Because access to CAPS is limited to CAD employees, there is little risk of other users inappropriately using or accessing CAPS information.

Section 7.0 Redress

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

Procedures for individuals to access their information, which may have been collected or maintained in CAPS or in another CBP system, are identified in the cited SORN(s). Requests for access to the information contained in an ROI can be made to CBP's FOIA Office via FOIAonline or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

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

Procedures to correct information collected or provided to CBP from the source systems are governed by the original system owner of the record repository from which information was sourced. For example, correction of e-QIP data requires submission of an updated e-QIP; correction of information contained within a credit bureau report requires the subject to contact the credit reporting company. CBP has quality control checks on information placed into CAPS, including a Quality Control team who reviews the data and information for accuracy. Pursuant to the Personal Security Management SORN,[19] requests for personnel security records are directed

[19] *See* DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), available at https://www.dhs.gov/system-records-notices-sorns. This SORN is in the process of being updated.

to the DHS or CBP FOIA Office, which maintains the accounting of record disclosures. Individuals may submit a written statement to CBP OPR PSD regarding any disputed information to be retained as part of the ISMS investigative record.

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

Individuals are notified of the procedures to correct their information at the point of collection through Privacy Act statements and other similar notices. Individuals submitting information to CBP electronically are provided with information about how to use e-QIP, including how to make corrections. That said, the ability to use e-QIP to correct information may be limited once the information is formally submitted to CBP, and any subsequent corrections would need to be routed to CBP OPR. In addition, subjects verify their information during the polygraph process. General notice is provided by the Personnel Security Management SORN and this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the individual will not be able to provide updated information to CBP if they believe any of the information maintained in CAPS is inaccurate.

Mitigation: This risk is mitigated. Most of the information contained in CAPS is self-reported by the individual undergoing a background investigation when he or she submits a completed e-QIP Questionnaire and other relevant documentation. An individual can correct erroneous information in e-QIP prior to submission. If the individual becomes aware of an error after submission, or believes any other information may be erroneous, he or she may contact the assigned human resources or personnel security point of contact.

Privacy Risk: There is a risk that inaccurate information that has been in a source system will remain inaccurate in CAPS.

Mitigation: This risk is partially mitigated. CAPS is not the official repository for the personnel security record, and there is no automated process to ensure that new or modified information in a source system is later updated in CAPS. The risks associated with this gap are mitigated by the fact that CAPS is only used in support of the polygraph process and for that particular period of the suitability process. Once the exam is completed and the suitability process completed, the information is maintained in CAPS for record keeping purposes, but any decisions are based on the information in the official personnel record.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

User access to the information in CAPS is authenticated via Active Directory. Access control is role-based, and data is restricted and will only be accessible if a specific user has a "need to know," has been approved for access to the data, and has met all training requirements. Periodic reviews are conducted on the application of user roles, and further administrative actions, such as granting access, removing access, or altering roles for those who already have access, are conducted by the CAD Management Staff.

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

All CBP employees and assigned contractor staff receive appropriate privacy and security training and have undergone necessary background investigations for access to sensitive, private, or classified information or secured facilities. CBP ensures this through legal agreements with its contractors, and enforcement of internal procedures with all CBP entities involved in processing the background checks. Additionally, robust standard operating procedures and system user manuals describe in detail user roles, responsibilities, and access privileges.

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

The following procedures are in place to ensure that access to information in CAPS is limited to authorized users:

- Access to CAPS requires a CBP Active Directory account, and requires the user to log into a CBP Intranet accessible computer;[20]
- A system access request must be completed, signed, and approved by the requester and requester's manager prior to the creation or distribution of personnel security data, to avoid accidental, inappropriate, or unauthorized use of the data;
- CAPS user accounts are individually approved by CAD Management staff before they are provisioned; and
- Access to information is role based and granted on a "need to know" basis when users of the system have access to a limited subset of data based on the concept of least

[20] Requirements for obtaining access to CBP Information Technology Systems are documented in CBP Handbook, HB 1400-05D, "Information Systems Security Policies and Procedures Handbook," version 6.01, dated May 17, 2016.

privilege/limited access.

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?

CBP establishes data sharing agreements with external entities using Interconnection Security Agreements. DHS Sensitive Systems Policy Directive 4300A, July 2017 establishes this requirement for DHS systems. An Interconnection Security Agreement is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Authorizing Official (AO). The Interconnection Security Agreement documents the security protections that must operate on interconnected systems. The MOU or contract documents acceptable uses of the information and access limitations. The Interconnection Security Agreement includes descriptive, technical, procedural, and planning information, and formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The AO for each organization is responsible for reviewing and signing the Interconnection Security Agreement.

Contact Official

Scott A. Stevens
Office of Professional Responsibility
U.S. Customs and Border Protection
(202) 344-1800

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

[Original signed copy complete and on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717