Privacy Impact Assessment
for

Cornerstone

DHS/CBP/PIA-038

February 27, 2017

Contact Point
Jerry Tavenner
Assistant Director
Personnel Security Division, Office of Professional Responsibility
(202) 325-7755

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) created the Cornerstone information management system to automate and manage the background investigation (BI) process for CBP employees, contractors, and applicants. Cornerstone facilitates the BI process by retrieving, compiling, and distributing information between several information systems during the BI process. CBP is conducting this Privacy Impact Assessment (PIA) because Cornerstone collects and maintains personally identifiable information (PII) about employees, applicants, contractors, and members of the public.

Overview

In support of the U.S. Customs and Border Protection (CBP) law enforcement and national security missions, the CBP Office of Professional Responsibility (OPR), Personnel Security Division (PSD) conducts background investigations (BI) on CBP applicants and employees (both federal and contractor) to determine their: 1) initial suitability/fitness for employment with CBP; 2) continued suitability/fitness for employment with CBP; 3) eligibility to occupy a national security position or access classified information; and 4) eligibility for access to federal facilities and/or information technology systems. The level of investigation required is determined by the sensitivity designation of the position applied for or occupied. This designation is established in accordance with Office of Personnel Management (OPM) guidance. OPM has delegated the authority to conduct BIs to CBP.[1] DHS has delegated the authority to CBP to make determinations as to an individual's suitability for employment or eligibility for access to classified information.[2]

CBP developed Cornerstone to facilitate a paperless BI process. Cornerstone retrieves, parses, compiles, packages, transmits, and attaches a variety of CBP applicant and employee information and documents. Information maintained within or passing through Cornerstone can be divided into three categories: 1) Record Identifiers (sensitive personally identifiable information (SPII) including name, Social Security number (SSN), and date of birth); 2) System Logs (a record of actions performed by Cornerstone, which may include SPII and other data needed to conduct the action); and 3) Record Information (all other investigative information, including secure database tables within Cornerstone, obtained as a result of data requests and queries). Cornerstone does not score, analyze, or create new information. Cornerstone is not a document repository, but does maintain sufficient data to perform a variety of functions.

The Background Investigation Tracking System (BITS), previously in development, was planned as a single point of access for users who desired the ability to centrally track information

[1] Memorandum of Understanding between U.S. Office of Personnel Management and U.S. Customs and Border Protection for Delegated Investigative Authority, signed March 11, 2015.
[2] DHS Delegation 12000, dated June 5, 2012, Delegation for Security Operations within the Department of Homeland Security.

in the system. It was intended to provide OPR with the ability to electronically create, track, manage documents and correspondence, and to communicate the status of background investigations throughout the BI lifecycle within OPR. Development for this system was halted, and BITS is currently not in use by CBP. However, if for any reason this changes, CBP will update this PIA.

CBP maintains Record Identifiers for a period not-to-exceed (NTE) 15 years.[3] CBP maintains System Logs and Record Information (including a variety of documents) for a sufficient period to ensure Cornerstone is able to complete its various functions as described below. CBP anticipates that System Logs and Record Information will generally be deleted within a year. The information captured by Cornerstone is discussed in more detail in Section 2.1.

Workflow

Applicants

The CBP Office of Human Resources Management (HRM), or other designated CBP office, initiates applicant BIs via email notification to the applicant of the BI requirement following acceptance of a tentative job offer.[4] The notification provides instructions for accessing OPM's Electronic Questionnaire for Investigations Processing (e-QIP)[5] system in order to complete and submit their BI package. The package consists of the Questionnaire for Investigations Processing and associated release forms, a Financial Disclosure Form (if applicable), and any other required documents. Additionally, the notification provides instructions for the applicant to submit his or her fingerprint charts. Within the e-QIP system, the applicant electronically releases the completed BI package to HRM and, after reviewing for completeness, HRM releases the BI package to OPR. Applicant fingerprints are collected in, or converted to, a digitized format and saved within Cornerstone. Using Cornerstone, HRM's Human Resources Business Engine (HRBE)[6] transmits sufficient applicant data to create a case within the DHS-owned Integrated Security Management System (ISMS),[7] which is the case management system OPR uses to track the background investigation and suitability determination process. ISMS also serves as the document repository for the BI and adjudication process.

[3] Legacy Department of Treasury-U.S. Customs Service Records Disposition Authority Job # N1-36-92-1, dated November 19, 1993.
[4] Only those applicants that have been extended this tentative offer will have their information used by Cornerstone.
[5] *See* Office of Personnel Management Electronic Questionnaires for Investigating Processing (e-QIP) PIA (August 2, 2007), *available at* https://www.opm.gov/information-management/privacy-policy/privacy-policy/eqip.pdf.
[6] *See* DHS/CBP/PIA-032 Human Resources Business Engine (HRBE) (July 25, 2016), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-hrbe-july2016.pdf.
[7] *See* DHS/CBP/PIA-038(a) Integrated Management System (ISMS) (September 16, 2014), *available at* http://www.dhs.gov/publication/dhs-all-pia-038a-integrated-security-management-system-isms. As applicable, requests/dates for polygraph examinations, polygraph results, and polygraph examination reports are processed entirely within ISMS and do not pass through, nor are stored within, Cornerstone.

Current Employees

Current employees (and contractors) are required to undergo periodic reinvestigation, or may be required to undergo an upgraded investigation if necessary for access to classified information. OPR initiates employee BIs via email notification to the employee of a BI requirement; the notification provides instructions for accessing OPM's e-QIP system in order to complete and submit his or her BI package (described above). If fingerprints are required, instructions are provided for the employee to obtain and submit fingerprint charts. Employee fingerprints are collected in, or converted to, a digitized format and saved within Cornerstone. The employee electronically releases the completed BI package to OPR, and OPR staff manually create a corresponding case in ISMS.

All Applicants and Employees

An extensible markup language (.xml) copy of the BI package is manually downloaded from e-QIP into Cornerstone and then saved in ISMS. Cornerstone then 1) prepares an e-QIP summary report; 2) requests preliminary vetting checks based on information within the questionnaire and generates a composite vetting check summary report containing the results of the vetting checks; 3) requests a Credit Bureau Report (CBR); and 4) queries the Selective Service System (if applicable) for registration data. The e-QIP Questionnaire (including associated release forms), the e-QIP summary report, the composite vetting checks summary report, the CBR, and the Selective Service check are uploaded to ISMS and attached to the relevant record. OPR manually releases the e-QIP Questionnaire to OPM within the e-QIP system and transmits the digitized fingerprint charts to OPM's Fingerprinting Transaction System (FTS)[8] via Cornerstone, thereby initiating the National Agency Check (NAC).[9] OPM then transmits an electronic copy of the e-QIP Questionnaire back to Cornerstone. Using Cornerstone's Intake Case Scheduler function, OPR staff assign each ISMS investigation case to an Investigative Service Provider (ISP)[10] to complete the investigation. Cornerstone's Electronic Package and Delivery function encrypts the investigative package and saves it within the CBP secure Message Queue (MQ)[11]

[8] Memorandum of Understanding between U.S. Office of Personnel Management Federal Investigative Services and U.S. Department of Homeland U.S. Customs and Border Protection for Access to the Fingerprint Transaction System (FTS), signed December 22, 2012.

[9] A National Agency Check is a required component of all background investigations. It consists of a query of national law enforcement databases for records associated with the subject. This includes queries of Social Security numbers, FBI investigative files, FBI criminal history files, and military records.

[10] CBP has established contracts with multiple ISPs to conduct BIs.

[11] Similar to a secured shared drive, a secure Message Queue (MQ) is within the CBP firewall protections but can be accessed by authorized non-CBP entities (i.e., ISPs). Each ISP is given restricted access only to its portion of the MQ in order to retrieve work assignments (investigation case packets) and return the completed work assignments to CBP.

where it can be accessed only by the assigned ISP.[12] The ISP then accesses the investigative package over a Virtual Private Network (VPN)[13] and uses it to complete the assigned investigation. This investigation package consists of the e-QIP Questionnaire (with associated releases), a CBR, a scheduling sheet (providing any specific investigation instructions),[14] a Financial Disclosure (if applicable), and a "For-Official-Use-Only" disclaimer. A copy of the complete investigative package is saved within ISMS. The ISP completes the investigation and through the VPN connection, saves the completed Report of Investigation (ROI) to the CBP MQ. Cornerstone retrieves the ROI from the CBP MQ and attaches it to the open case file for the individual within ISMS for review and adjudication by OPR adjudicators. HRBE transmits requests to Cornerstone for the status of BI cases on a daily basis. Cornerstone then sends the request to ISMS for the status information and provides the results back to HRBE.

Internal System Connections

Cornerstone connects directly with CBP Cloud Computing and CBP Directory Service systems. Cornerstone is a virtual server that operates within a cloud environment. It uses the CBP Directory Service to authenticate user access within the active directory. Cornerstone exchanges information with HRBE through an automated interface called a web service, which is self-contained and secure. Cornerstone uses this data to create a corresponding case within ISMS and to provide updated BI status information to HRBE.

Cornerstone also exchanges information with ISMS[15] via web service. ISMS serves as the DHS enterprise repository for personnel security data. It is used to manage the suitability decisions and security clearance determinations for employees, contractors, detailees, and state and local partners. DHS mandated the use of ISMS by all DHS components, including CBP. Cornerstone transmits formatted secure messages to ISMS; these messages contain the data and documents gathered or updated during the investigative process.

Historically, Cornerstone exchanged information with CBP Vetting, a service that allows authorized users to query and receive data from the National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (Nlets), Currency or Monetary Instruments Report (CMIR), Search/Arrest/Seizure (S/A/S) report, and TECS[16] via the CBP MQ.

[12] The ISP does not have access to ISMS or Cornerstone. However, for accurate recordkeeping, once the package is transmitted to the ISP via the Message Queue, a copy is maintained in ISMS and Cornerstone.
[13] A VPN is a secured connection between two points through which information and documents can be sent.
[14] Scheduling is the process of transmitting a request for a background investigation to one of OPR's Investigative Service Providers.
[15] ISMS is accessed by OPR staff; limited read-only access is also provided to the Human Resources Office and the Freedom of Information Act Office based on a specific need to know.
[16] TECS (not an acronym) is the updated and modified version of the former Treasury Enforcement

Encrypted e-QIP data was sent by Cornerstone to CBP Vetting to query these data sources. Cornerstone compiled the results into a vetting checks summary report that it then attached to ISMS. In January 2017, OPR replaced this process with the use of the Employee and Applicant Suitability and Eligibility module (EASE) within the Automated Targeting System (ATS).[17] ATS-EASE facilitates automated queries of a number of systems, including TECS. Unlike results obtained through CBP Vetting, results of the ATS-EASE checks will not be retained in Cornerstone.

External System Connections

1) USA Staffing: Although there is no direct connection between Cornerstone and USA Staffing, the majority of the PII received, maintained, or transmitted through Cornerstone is initially provided by the subject when he or she submits an application for a job via OPM's USA Staffing system. Individuals applying for federal employment provide their name, date of birth, Social Security number, address, and phone number, which is then transmitted to HRBE and subsequently via Cornerstone to ISMS.

2) e-QIP: Although there is no direct connection between Cornerstone and e-QIP, additional information, which eventually passes through Cornerstone, is provided by the subject of an investigation via e-QIP. The e-QIP system offers a secure environment by which an individual provides the information required for a BI. Applicants and employees access e-QIP over a secure Internet connection using widely-available web browsers. OPM's e-QIP then sends the information to CBP through a secure VPN connection between OPM and CBP, using internal (non-internet-based) email. This is a one-way connection from OPM to CBP. The data is encrypted with FIPS 140-2 compliant methods. Cornerstone retrieves the email automatically and captures all information necessary to conduct comprehensive BIs on an individual from the subject application data provided by e-QIP. Cornerstone uses this data to perform vetting checks, request a CBR, and to query the Selective Service System, if necessary, to obtain relevant investigative material.

3) Virtual Private Network (VPN): These connections are used to exchange information

Communications System. TECS, owned and managed by DHS/CBP, is the principal system used by CBP officers at the border to assist with screening and making determinations regarding admissibility of arriving persons as Suspicious Activity Reports (SAR) for inclusion in the National SAR Initiative (NSI), which is led by the Department of Justice on behalf of the entire Federal Government. *See* DHS/CBP/PIA-009 TECS (August 15, 2011), *available at* https://www.dhs.gov/publication/tecs-system-cbp-primary-and-secondary-processing-tecs-national-sar-initiative.

[17] For additional information on ATS-EASE, please *see* DHS/CBP/PIA-006(e) Automated Targeting System (ATS) PIA Update (January 13, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-006-e-ats-january2017.pdf.

between OPR and ISPs. An investigative package is created for each case and forwarded to an ISP. The data is encrypted and saved to the CBP MQ. The ISPs access the CBP MQ via secure VPN to retrieve the package and to save the completed ROI within the CBP MQ. An Interconnection Security Agreement has been signed between CBP and each ISP to document the connection. ISP contractors are required to have and maintain a favorably adjudicated Single Scope Background Investigation (SSBI)/Tier 5 level investigation[18] to ensure they properly protect the information. Once completed, Cornerstone retrieves the ROI from the CBP MQ and attaches it to the case file in ISMS. OPR staff use the information in ISMS to complete the adjudication of the BI.

4) OPM Fingerprinting Transaction System (FTS) connection: Cornerstone packages the digitized fingerprint charts and uses internal (non-internet-based) email to send the package to OPM through a secure VPN connection between CBP and OPM. This is a one-way connection from CBP to OPM and the data is encrypted with FIPS 140-2 compliant methods.

Cornerstone is not considered an original source data system, nor does it create any new information. Its function is to assemble information and documents from other sources and then automate the dissemination and storage of that information into the appropriate record repository. All subject PII (e.g., record identifiers) is obtained directly from the subject via other source systems of records. All investigative information (i.e., record information), other than the ROI and fingerprint charts, is obtained from other source systems of records. System log information (which may include record identifiers) that tracks system activity does not generate any new information associated with the subject. The PII contained within Cornerstone consists of data elements necessary to identify the individual, perform automated vetting checks and system queries, schedule and receive BIs from ISPs, and track Cornerstone activity.

Other than as described in this PIA, CBP will not disclose information directly from Cornerstone. Such information must be specifically requested following strict information disclosure procedures, and only then will information be shared based on the disclosure provisions of the source systems or the official record repositories from which the information originated.

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?

[18] Effective October 1, 2016, Tier 5 investigations were implemented throughout the Federal Government. The Tier 5 level investigation replaced the former SSBI as the most in-depth investigation conducted for federal employment purposes. *See* OPM Federal Investigations Notice 16-07, dated September 26, 2016, "Implementation of Federal Investigative Standards for Tier 4, Tier 4 Reinvestigation, Tier 5, and Tier 5 Reinvestigation."

Cornerstone does not collect information directly from applicants, employees, or contractors. Rather, Cornerstone retains information collected by HRBE, OPM (via e-QIP), and TECS (via CBP Vetting, and now ATS-EASE) based upon the following authorities:

- 18 United States Code (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.
- Executive Order (E.O.) 10450 (May 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.
- National Security Information 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.
- E.O. 9397 (November 18, 2008) – Numbering. System for Federal Accounts Relating to Individual Persons, as amended by E.O. 13478, Amendments to E.O. 9397 Relating to Federal Agency Use of Social Security Numbers.
- 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.
- E.O. 10577 (November 23, 1954) – Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service.

- DHS Management Directive (MD) 121-01 (February 6, 2014) – assigns authority for DHS security programs to the 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 supporting DHS' security functions;
- 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 Cornerstone is covered by the following System of Records Notices (SORN):

- DHS/ALL-023 Personnel Security Management System of Records[19] provides CBP with the authority to collect and maintain 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[20] provides CBP with the authority to collect 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.

1.3 Has a system security plan been completed for the information systems supporting the project?

A system security plan has been completed for Cornerstone, and a security certification authorizing the Authority to Operate was granted on March 13, 2014, by the CBP Information

[19] *See* DHS/ALL-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.
[20] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-11-27/html/2012-28675.htm.

Systems Security Manager Certifying Official. The Cornerstone Federal Information Security Management Act (FISMA) ID is CBP-06290-MAJ-06290.

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

In general, Cornerstone is covered by a legacy[21] U.S. Customs Service NARA-approved Records Disposition Authority Job Number N1-36-92-1 certified on November 9, 1993, Personnel Security Clearance Files. This authority was further documented in legacy U.S. Customs Service Record Retention Handbook, CIS HB 2100-05A, dated January 2001.

Various types of records are created and maintained during the course of the hiring process to assist the entrance of an employee into the 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. 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.

Cornerstone does not collect information directly from an individual, and therefore these systems are not covered under the PRA. However OPM does collect information directly from an individual via e-QIP using Standard Forms (SF): SF-85, SF-85P, or SF-86,[22] 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.

[21] Prior to 2001, the U.S. Customs Service was a component of the U.S. Department of Treasury. As this NARA-approved Records Disposition Authority (Job Number N1-36-92-1) was implemented prior to the establishment of DHS and CBP, Cornerstone is covered under this legacy schedule.
[22] 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 maintained within or passing through Cornerstone can be divided into three categories of information: 1) Record Identifiers (SPII including name, SSN, date of birth), 2) System Logs (a record of actions performed by Cornerstone, which may include SPII), and 3) Record Information (all other investigative information obtained as a result of data requests/queries). The information Cornerstone collects and maintains is necessary to identify an individual and initiate suitability and personnel security related processes.

Cornerstone collects and maintains elements of PII/SPII, including:

- First Name
- Last Name
- SSN
- Address
- Date of Birth
- Place of Birth
- Citizenship Country
- Gender
- Document Number

System Logs created and maintained include the following non-PII:

- Codes (including transaction codes, document type codes, and investigation type codes)
- Dates (dates that checks were performed, dates for cases scheduled, and dates ROIs were received)

Investigative information that passes through Cornerstone includes the results of the investigative queries and reports described above. Additionally, Cornerstone temporarily maintains the following documents within a secure directory pending verification of successful attachment to the case file in ISMS and the scheduling of the investigation to the ISP.

- e-QIP Questionnaire and associated releases
- e-QIP Summary Report

- Financial Disclosure Form
- Scheduling Sheet
- Vetting Check Summary Report
- CBR (name, last 4 digits of the SSN, address, and all associated financial information found on the credit report)
- Selective Service Registration Results
- e-Fingerprint Chart (digitized)
- ROI

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

E-QIP

All selected applicants and employees complete and submit an e-QIP Questionnaire within OPM's e-QIP system. After review by CBP OPR, an extensible markup language (.xml) copy of the BI package is manually downloaded into Cornerstone. Cornerstone parses the .xml copy of the Questionnaire and captures pertinent information it needs to perform the preliminary vetting checks for relevant investigative material, and query the Selective Service System and CBR commercial data providers. The e-QIP Questionnaire is also systemically released to OPM within the e-QIP system. For the purpose of delegated investigations[23] (i.e., an agency's ability to make specific inquiries concerning an applicant's criminal or credit background), OPM also sends the e-QIP form information to CBP through a secure VPN connection between OPM and CBP, using internal (non-internet-based) email. This is a one-way connection from OPM to CBP and the data is encrypted with FIPS 140-2 compliant methods. Cornerstone retrieves the e-mail and attaches the e-QIP to the case file in ISMS.

Investigative information

Cornerstone requests/submits the following information using Hyper Text Transfer Protocol Secure (HTTPS) web services:

- *Credit Bureau Reports (CBR)* – A review of the applicant or employee's credit history is used to determine whether or not the individual is in good financial standing and if he or she could pose a potential security risk. Via Web Services

[23] For more information about OPM's delegation authorities to agencies, see Title 5, C.F.R., Part 731.103 – Delegation to Agencies, specifically (d)(1) (https://www.gpo.gov/fdsys/granule/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-103); and §731.102 Implementation.

over HTTPS, Cornerstone requests CBRs from a DHS-contracted commercial data provider that maintains this information; the CBR includes information from all three major credit reporting bureaus.[24] Cornerstone will maintain the date the CBR was requested by CBP in a secure database table. Cornerstone attaches the received CBR to the case file in ISMS. The CBRs are not stored in Cornerstone.

- *Selective Service System*[25] – Cornerstone requests Selective Service registration verification from the Selective Service System. Data received are Yes-registered (registration number) or Not Registered. This information is used to verify that males undergoing an investigation who are required to register with the Selective Service System, have registered. Women are not required to register so there is no option to query on females. Cornerstone maintains the date the Selective Service check was requested by CBP in a secure database table within Cornerstone. Cornerstone attaches the Selective Service check to the case file in ISMS; information provided back includes whether the individual is registered or not, and if so, the registration number.

Cornerstone also exchanges information with two web-based DHS systems:

Integrated Security Management System (ISMS) – ISMS is a DHS web-based case management tool. It is designed to support the lifecycle of DHS personnel security, administrative security, and classified visit management programs. Personnel security records maintained in ISMS include suitability and security clearance investigations, which contain information related to background checks, investigations, and access determinations. The system is a DHS enterprise-wide application. Cornerstone sends person information, position information for the vacancy, and investigation status information to ISMS. Cornerstone also automatically attaches documents to ISMS records.

Human Resources Business Engine (HRBE) – HRBE is an HRM web-based workflow and process tracking tool that simplifies the hiring process by automating hiring procedures using a single, unified underlying database. Applicant personal data is collected indirectly from the subject via HRBE. When applying for employment, applicants/employees enter their personal data into OPM application forms (via USA Staffing), which is transmitted to HRBE and, if the applicant is selected for employment, the data is subsequently transmitted through Cornerstone to ISMS.

[24] The three major credit reporting agencies (also sometimes referred to as credit bureaus) are Experian, TransUnion, and Equifax.
[25] More information about the Selective Service System can be found at: https://www.sss.gov/.

Cornerstone retains the following information via connections with OPM and TECS (for historical records containing results from CBP Vetting, no longer in use):

- *Fingerprint Checks* – Cornerstone submits to OPM requests for fingerprint checks using the Integrated Automated Fingerprint Identification System (IAFIS)[26] through the OPM FTS. FTS accepts electronic submissions from CBP to request fingerprint checks through FBI Criminal Justice Information Services. The data is exchanged through a secure VPN connection between OPM and CBP utilizing internal (non-internet-based) email. The data is encrypted with FIPS 140-2 compliant methods. OPM returns the results of the fingerprint check to CBP via e-Delivery directly into ISMS and subsequently returns the results again as part of the composite NAC directly to ISMS. Cornerstone maintains the date the fingerprint check was requested by CBP and the captured fingerprint card in a secure database table. Cornerstone updates ISMS with the date the fingerprint card was received and verifies that it was received electronically.
- *TECS/National Crime Information Center (NCIC)/National Law Enforcement Telecommunications System (Nlets)* – CBP now uses ATS-EASE as it offers a more robust search engine (e.g., improves efficiency) and additional functionality. Cornerstone submits law enforcement checks against TECS, NCIC, and Nlets. Law enforcement information, criminal history records, or outstanding warrants for an individual are collected and compiled into a vetting check summary report and attached to the case file in ISMS. Cornerstone also maintains the date when CBP requested the TECS/NCIC/Nlets checks in a secure database table within Cornerstone. Cornerstone attaches these checks to the case file in ISMS.

Investigative Service Providers (ISPs) – ISPs are investigative companies that have contracts with OPR to perform BIs. CBP requests an ISP perform a BI and provides them with required information as previously described. The ISP saves the completed ROI to the CBP MQ. Cornerstone retrieves the ROI from the CBP MQ and attaches it to the case file in ISMS. Cornerstone maintains the date the ROI was provided in a secure database table.

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

As described above, Cornerstone uses credit bureau report information from commercial

[26] Fingerprint Checks are a subset of the National Agency Check (NAC). For more information about privacy policies related to FBI's IAFIS, please *see* Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements, *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis.

data providers. Cornerstone attaches the CBR to the personnel security record in ISMS, and maintains the date the CBR was requested in a secure database table within Cornerstone.

2.4 Discuss how accuracy of the data is ensured.

PII maintained in or passed through Cornerstone is initially provided by the subject through other systems (USA Staffing, HRBE, and e-QIP). Individuals are provided an opportunity to review the information and must certify it is accurate prior to submission to these other systems.

Investigative data is obtained from a variety of sources listed above. Adjustments or corrections to this information must be made through the source system (e.g., corrections to a CBR must be made through the credit reporting company). The information as passed through Cornerstone is an accurate reflection of the information received. Opportunities to review or correct the accuracy of the information stored within ISMS or the source systems are contingent upon the provisions of those systems.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is the possibility of human data entry error resulting in data being associated with the wrong individual within Cornerstone (e.g., subject error when entering personal information into e-QIP or USA Staffing, or the accidental swapping of an investigation case number during scheduling).

Mitigation: This risk is mitigated by several factors. If the subject erroneously enters personal information into e-QIP, it is returned to the subject for correction. Upon resubmission, Cornerstone will replace/overwrite the erroneous data. There is no opportunity to correct erroneous personal information (provided by the subject) within Cornerstone, it must be corrected in the source system and/or in the record repository (ISMS).

Automated data association is used to the greatest extent possible to minimize the potential for human data errors (for example, Cornerstone uses applicant-provided SPII to obtain associated investigative material without further human intervention).OPR staff are trained to exercise care when scheduling cases to minimize the potential for data entry error (e.g., "swap" of case numbers). In the event such an error occurs, OPR staff reschedule the case with the correct information, and notification is provided to the ISPs (external to Cornerstone) to correct the scheduled work. The erroneous record information within Cornerstone is then deleted by OPR staff. Additional redress opportunities for ISMS are available to the individual as outlined in the DHS/ALL-023 Personnel Security Management SORN,[27] and Sections 1.2 and 7.0 of this PIA.

[27] *See* DHS/All-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Cornerstone uses the information to facilitate the completion of suitability and personnel security processes, including background or other investigations of an individual. As described in Section 2.1, PII is collected to clearly identify, track, and associate records with a specific individual during the suitability or security clearance processes (record identifiers). Documents temporarily maintained within Cornerstone are used to facilitate the scheduling of investigative requirements. In addition to the documents provided to the ISPs as part of the investigation package (as described in Section 2.1), Cornerstone acts as a temporary document repository for the digitized fingerprint charts until they are released, along with the e-QIP Questionnaire, to OPM as described above.

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.

Data in Cornerstone is used to collect and send security-related information through the BI case flow process. There is no built-in analysis functions to identify patterns, anomalies, or new areas of concern.

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

Cornerstone is only accessed by authorized CBP employees (including contractors) based on assigned roles. CBP employee access to Cornerstone data is authenticated via Active Directory. Access control is role-based, and data is only accessible if a specific user has been approved for access to the data.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There are privacy risks associated with the handling of PII that may occur when data is extracted from Cornerstone if the individual using the data improperly distributes or stores the data.

Mitigation: To address these risks, the following controls and mitigation strategies are in place to handle PII:

- Access to Cornerstone requires a CBP Active Directory account and requires the

user to log into a CBP Intranet-accessible computer;[28]

- A system access request must be completed, signed, and approved by the requester and requester's manager prior to the creation and distribution of personnel security data to avoid accidental, inappropriate, or unauthorized use of the data;
- Cornerstone user accounts are individually approved by PSD Support Services 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 privilege/limited access.
- As contractor employees separate, OPR is notified and the contract employee's access to Cornerstone is terminated. OPR is also notified at the end of each pay period of all CBP employees who have separated and their access is terminated.
- OPR requires supervisory recertification on an annual basis of each employee's continued need for access to Cornerstone.

Privacy Risk: There are privacy risks associated with system security regarding "insider threat," when an individual with authorized access to the system conducts unauthorized activities (e.g., attempting to access or disclose information for which he or she does not have permission).

Mitigation: To address this risk, the following system security controls and mitigation strategies are in place:

- A system security certification is performed and obtained in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources.
- Cornerstone undergoes a monthly security scan(s), which include vulnerability checks and identification/reports of any unapproved software. Cornerstone also has a de-provision process to remove access upon notification of change in employment status or position and removes user access.
- All automated data processing equipment supporting the application environment is located in a secure DHS data center.
- When information is stored as an attachment on the server, file/folder access is restricted by file/folder permission to prevent access by those without a "need to

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

know."

- Specific security roles are defined and implemented within the application to control access to information.

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.

Cornerstone receives all of its information directly or indirectly from other sources (including e-QIP, USA Staffing, HRBE, credit bureaus, and the Selective Service System). In every instance, an individual must apply for employment, receive a tentative offer of employment (or be a current employee or contractor), and complete an e-QIP form that provides the collection notice required by the Privacy Act, 5 U.S.C. § 552a(e)(3). The Privacy Act Statement 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 an ROI), and submits to a named-based threat background check commensurate with the sensitivity of the position.

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

An individual receives notice via e-QIP at the beginning of the background investigation process that describes how the information will be used and advises that submission of the information is voluntary. The individual may opt-out of providing information; however, if the information is not provided, the individual will not meet suitability requirements and may be deemed ineligible for federal employment. Individuals are informed of how the information will be used upon submission of the e-QIP through the OPM Privacy Act Statement on the application.[29] The e-QIP form includes authorizations for specific disclosures, including: 1) a Fair Credit Reporting Disclosure and Authorization; 2) an Authorization for Release of Medical

[29] Additional information about OPM's Freedom of Information Act (FOIA) and Privacy Act policies can also be found at: https://www.opm.gov/investigations/e-qip-application/#60c.

Information; and 3) a General Authorization for Release of Information, which serves as authorization to conduct the investigation. Each of these forms must be signed and submitted by the subject of the BI.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that their information is housed in Cornerstone and ISMS.

Mitigation: The individual receives notice from the source agency at the time of collection regarding the general purpose and use of his or her information via the Privacy Act Statement. As previously noted, individuals submit signed releases that authorize the release of information pursuant to the investigation, release of credit bureau information, and release of medical information. Although Cornerstone is not specifically identified in these statements and disclosures, the individual does receive notice that his or her information may be used to perform BI functions as part of the overall employment or re-investigation process.

In addition, this PIA, the ISMS PIA, and related SORNs, all published to the DHS public website, provide additional notice of the use, maintenance, and re-dissemination of information.

Section 5.0 Data Retention by the project

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

In general, Cornerstone is covered by a legacy U.S. Customs Service NARA-approved Records Disposition Authority Job Number N1-36-92-1, certified November 9, 1993, Personnel Security Clearance Files. This authority was further documented in legacy U.S. Customs Service Record Retention Handbook CIS HB 2100-05A, dated January 2001, and provides for retention of Personnel Security Clearance records for up to 15 years. Cornerstone is not a document repository, but does maintain sufficient data to perform a variety of functions. Record Identifiers are maintained for a period not-to-exceed (NTE) 15 years. System Logs and Record Information (including a variety of documents) are maintained for a sufficient period to ensure Cornerstone is able to complete its various functions as described above. It is anticipated that System Logs and Record Information will generally be deleted within one year. At the time of publication of this PIA, data is manually deleted from Cornerstone after verification that Cornerstone has completed its various processes (including attachment of documents to the case file in ISMS). An automated disposal process for Record Information and System Logs is in development.

ISMS remains the enterprise repository for personnel security records and is subject to the retention periods described in General Records Schedule 18, items 22-25.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk associated with the retention of information in that the data will be retained beyond the requirements established in the records retention schedule.

Mitigation: This risk is partially mitigated. As noted above, until an automated disposal process for Record Information and System Logs in Cornerstone is developed, data is manually deleted from Cornerstone after verification that Cornerstone has completed its various processes (including attachment of documents to ISMS). Efforts to automate this disposal process are in development. All other information is retained for 15 years.

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.

Yes. Information shared outside of DHS is described in Section 2.2. Cornerstone shares information with only those external recipients necessary to complete the BI processes and receive the ROIs. In addition, information such as names, SSNs, and dates of birth may be shared with the owners of specific types of information in order to secure, for example, credit reports, Selective Service registration verifications, citizenship and immigration checks, fingerprint checks, and criminal history checks.

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

The external sharing described in Sections 2.2 and 6.1 is compatible with the Personnel Security System of Records Notice,[30] pursuant to 5 U.S.C. § 552a(b)(3) as routine uses:

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees; and

H. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security

[30] *See* DHS/All-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

Cornerstone shares information with only those external recipients necessary to complete the BI processes and receive the ROIs. This sharing helps CBP ensure that individuals are eligible to receive a clearance.

6.3 Does the project place limitations on re-dissemination?

External agencies may request background investigation information from CBP.[31] CBP may transmit information or files that were received by or sent through Cornerstone, but may only transmit information sourced by CBP during the investigation (e.g., CBRs, ROIs maintained in ISMS). Such requests are processed based upon re-dissemination limitations and restrictions outlined in sharing agreements, which describe how requests are to be submitted, contain a list of those who are authorized to request such information, provide what may be shared, and the applicable limitations and restrictions. Re-dissemination of the shared information must remain compatible with the reason for which the information was originally collected, and must remain compatible with the reasons outlined in the sharing agreements.

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

Cornerstone maintains a system log of all information shared from Cornerstone with external sources. Disclosure records for information collected or passed through Cornerstone and subsequently disclosed from a record repository (e.g., ISMS) are maintained in accordance with disclosure requirements of that repository. As identified in the cited SORN, requests for personnel security information from those repositories are made to CBP's Freedom of Information Act (FOIA) Office via FOIAonline[32] or through the process outlined in Section 7.1. The CBP FOIA Office maintains an accounting of records disclosed, when, and to whom.

6.5 Privacy Impact Analysis: Information Sharing

Privacy Risk: There is a risk that an external source with whom information is shared could retain, use, or release PII from Cornerstone in an unauthorized manner.

Mitigation: To address this risk, the following controls are in place:

- ISP contractors must have received a favorably adjudicated SSBI/Tier 5

[31] *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.

[32] A FOIA request can be made government-wide via FOIAonline at: https://foiaonline.regulations.gov/foia/action/public/request/publicPreCreate#.

investigation, and receive internal annual refresher training provided by the ISP on the proper use of PII. Contractual requirements provide for the limited use of the information the ISPs receive and how it may be stored and accessed. Additionally, periodic audits are conducted at ISP locations to confirm contractual requirements are followed.

- The Memorandum of Understanding (MOU) between OPM and CBP for access to the FTS establishes the security controls and responsibilities associated with the uses of fingerprint information.
- Contractual requirements with the CBR provider limit the use of the data shared.

Section 7.0 Redress

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

With the exception of the ROI and fingerprint charts, Cornerstone contains no new or source records associated with individuals. Procedures for individuals to access their information, which may have been collected or passed through Cornerstone and subsequently maintained in ISMS are identified in the cited SORN(s). Requests for access to the information contained in the 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. Since Cornerstone is not a source system nor a permanent record repository for any information, there is no option for the individual to correct information maintained within Cornerstone. Any "corrective" action would need to be done with the host record repository. All of the information collected and passed through Cornerstone is maintained

in ISMS. Pursuant to the Personal Security Management SORN,[33] requests for personnel security records are made to the DHS 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?

As noted above, there is no option for the individual to correct information maintained within Cornerstone. Any corrective action would need to be done with the host record repository. Consequently, Cornerstone does not provide such notice.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A potential risk associated with redress concerns the ability to validate the accuracy of the information being reviewed.

Mitigation: Most PII contained in Cornerstone is self-reported by the individual undergoing a BI when he or she submits a completed e-QIP Questionnaire. An individual can correct erroneous information in e-QIP prior to submission. If the individual becomes aware of an error after submission, he or she may contact the assigned human resources or personnel security point of contact or follow the redress procedures for e-QIP.

Privacy Risk: There is a risk that inaccurate information that has been corrected in e-QIP will remain inaccurate or out-of-date in Cornerstone.

Mitigation: Cornerstone maintains data as it was submitted through e-QIP and is an accurate reflection of that submitted data. If e-QIP data is subsequently corrected and passed through Cornerstone, the new data will overwrite any existing data maintained in Cornerstone and also be passed to ISMS. As previously noted in Section 7.3, erroneous data must be corrected in the source system.

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 Cornerstone is authenticated via Active Directory. Access

[33] *See* DHS/All-023 Personnel Security Management System of Records, 75 FR 8088 (February 23, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-02-23/html/2010-3362.htm.

control is role-based, and data 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 to, removing access, or altering roles for those who already have access, are conducted by the PSD Support Services 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, privacy, 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 Cornerstone is limited to authorized users:

- Access to Cornerstone requires a CBP Active Directory account, and requires the user to log into a CBP Intranet accessible computer;[34]
- 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;
- Cornerstone user accounts are individually approved by PSD Support Services 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 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

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

system by organizations within DHS and outside?

CBP establishes data sharing agreements with external entities using Interconnection Security Agreements. DHS 4300A, Sensitive Systems Policy Directive, April 2014, 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.

Responsible Officials

Kathleen L. Claffie
Acting CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

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

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security