



Privacy Impact Assessment  
for

**HRM 5000**

**DHS/CBP/PIA-055**

**July 11, 2018**

**Contact Point**

**Suzanne Shepherd**

**HRM 5000/Enterprise Services**

**U.S. Customs and Border Protection**

**(202) 863-6162**

**Reviewing Official**

**Philip S. Kaplan**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## Abstract

The U.S. Customs and Border Protection (CBP) Office of Human Resources Management (HRM) has selected contract support to improve and streamline the recruiting, hiring, and personnel security processes for CBP “Frontline” positions, including U.S. Border Patrol Agents, CBP Officers, and Air and Marine Interdiction Agents. HRM 5000 is CBP’s contract with Accenture Federal Services (AFS) LLC. This contract addresses surge hiring to support the President’s Executive Order for an additional 5,000 Border Patrol Agents (BPA). It will also be used to support the hiring of additional law enforcement positions within the Office of Air and Marine and the Office of Field Operations. CBP is publishing this Privacy Impact Assessment (PIA) because HRM 5000 requires AFS to collect, use, and retain personally identifiable information (PII) belonging to members of the public on behalf of CBP, as well as to identify and mitigate privacy concerns associated with the program as a whole.

## Overview

On January 25, 2017, the President issued the Border Security and Immigration Enforcement Improvements Executive Order,<sup>1</sup> and provided direction to CBP to take appropriate actions to recruit and hire individuals for critical frontline law enforcement positions. CBP HRM is committed to recruiting and retaining a world-class law enforcement workforce as a top mission support priority, and in support of the Executive Order, CBP solicited contract support to assist the CBP Hiring Center in meeting its challenging recruitment goals.<sup>2</sup> As part of the contract solicitation, CBP placed an aggressive focus on educating the public on CBP’s mission and the process of being hired for a CBP frontline position. CBP requires this level of outreach, marketing, and applicant support because the process for becoming a CBP frontline law enforcement officer can be lengthy, and many interested and well-qualified candidates are deterred from waiting for the outcome of the CBP hiring process.

There is intense competition for a shrinking pool of candidates, and a need for a large volume of interested and well-qualified applicants to maintain congressionally-mandated staffing levels. These requirements created the need for CBP to seek the services and expertise of industry to assist with its recruitment and hiring mission to protect America’s borders. CBP required

---

<sup>1</sup> Executive Order 13767: “Border Security and Immigration Enforcement Improvements,” (January 25, 2017), “Sec. 8. Additional Border Patrol Agents. Subject to available appropriations, the Secretary, through the Commissioner of U.S. Customs and Border Protection, shall take all appropriate action to hire 5,000 additional Border Patrol agents, and all appropriate action to ensure that such agents enter on duty and are assigned to duty stations as soon as is practicable;” available at <https://www.whitehouse.gov/presidential-actions/executive-order-border-security-immigration-enforcement-improvements/>.

<sup>2</sup> See U.S. Customs and Border Protection (CBP) National Recruitment & Hiring, Solicitation Number: HSBP1017R0029, available at <https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=71bb24db921980ad185f11c93cdf304e&cvi=0>.



requisite recruitment, market research, data analytics, advertising, and marketing services to be performed by a contractor with the experience and capability to execute a recruiting and hiring campaign to meet CBP staffing requirements on expedited timelines.

Accordingly, on July 7, 2017, CBP issued a statement of objectives<sup>3</sup> as part of its solicitation for contract support to provide: expert market research, data analytics, recruitment, and advertising expertise aimed at applicants for law enforcement opportunities within CBP. The contractor must also possess knowledge of the CBP law enforcement applicant processing path, systems integration skills, and demonstrated experience necessary to perform the full range of law enforcement talent acquisition processes.

Based on the statement of objectives and subsequent responses to a request for proposal, CBP issued a performance-based contract to Accenture Federal Services (AFS) LLC that emphasized the importance of delivering results rather than merely performing tasks. Payments to AFS are based on performance only. Ultimately, the goal is to produce the required number of applicants who actually enter on duty—which means, individuals who have completed the application, who have successfully passed the entrance exam, who meet physical requirements, who are suitable for employment at CBP (i.e., who can pass a very demanding background investigation, pass a polygraph examination, and have the highest integrity), and who are compatible with the rigors of training and the operational environments associated with frontline law enforcement positions.<sup>4</sup> AFS must recruit enough highly qualified frontline candidates to successfully satisfy the Executive Order over the course of the contract.<sup>5</sup>

To meet these aggressive recruiting goals, the contract requires AFS to incorporate “a hard-hitting, targeted recruitment campaign that consists of promoting the CBP law enforcement careers and opportunities while educating and guiding the potential candidates through the hiring process.” AFS will employ data analytics, targeted marketing and recruiting, technology innovations, call center support, additional specialized recruiting and human resources skillsets, and internal process improvements in meeting the demands required to achieve the aforementioned recruitment and hiring goals.

---

<sup>3</sup> See U.S. Customs and Border Protection (CBP) National Recruitment & Hiring, Statement of Objectives for HSBP1017R0029 (July 7, 2017), available at [https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=71bb24db921980ad185f11c93cdf304e&\\_cvi=0](https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=71bb24db921980ad185f11c93cdf304e&_cvi=0).

<sup>4</sup> Currently, more than 133 initial applicants must be recruited in order to successfully hire and place one Border Patrol Agent (BPA).

<sup>5</sup> This contract is one base year with 4 option years to hire 7,500 fully qualified applicants. These qualified applicants include 5,000 Border Patrol Agents (BPAs), 2,000 CBP Officers, and 500 Air and Marine Agents. Ultimately, remuneration to the contractor will be based primarily on the delivery of qualified applicants, as demonstrated by successful completion of all elements of the hiring process.



## HRM 5000 Objectives

CBP has issued four substantive high-level objectives for AFS to successfully meet the requirements of the contract.

1. **Recruiting.** AFS will expand the diversity of CBP frontline applicants by targeting recruitment efforts both locally and nationally. AFS will use data analytics to drive CBP recruitment marketing and advertising strategy. To meet CBP's challenges to recruit, hire, and retain qualified talent for frontline law enforcement occupations, AFS plans to increase its outreach to candidates, target a larger geographic footprint, and connect with diverse groups including women, minorities, and veterans. AFS will use digital recruitment strategies, increase its use of social media and targeted campaigns, as well as traditional advertising methods to achieve these goals, monitor candidate progress in real time, engage proactively via multimedia tools, and create candidate profiles. CBP's hiring process will benefit from multiple capability enhancements: data analytics, targeted marketing and recruiting, technology innovations, call center support, additional specialized skillsets, and process improvements. CBP expects that AFS best practices and improved processes will help to reduce time to hire for all applicants, and increase the total number of hires.
2. **Independently post Vacancy Announcements.** AFS will essentially create a new application intake system that complies with federal system requirements, interfaces with U.S. Office of Personnel Management's (OPM) USAJOBS system,<sup>6</sup> and can be integrated with CBP's Integrated Hiring System (IHS). AFS will prepare new job opening announcements (JOA) using CBP-approved templates that include all appropriate and required Agency criteria, including links to information that may be hosted by one or more other contractors or the Federal Government. AFS will determine whether applicants meet eligibility requirements based on their application responses. Certain determinations made initially by automated processes must be confirmed by manual review, in compliance with CBP HRM required procedures.
3. **Applicant Support/Care.** AFS will provide a system to monitor candidate progress throughout the hiring process for both CBP stakeholders and applicants. This new information technology system will provide a snapshot of the number of eligible candidates for each major step in the hiring process, the current JOA status (open or closed), and the date(s) the last announcement(s) were open.
4. **Application Intake and Applicant Processing.** AFS and CBP will manage the full life cycle of the hiring process from job posting to processing new entry-level frontline

---

<sup>6</sup> See OPM/GOVT/PIA – USAJobs (September 15, 2005), available at <https://www.opm.gov/information-management/privacy-policy/privacy-policy/usajobs.pdf>.



hires. CBP will retain all steps that are considered inherently governmental functions. The CBP Office of Professional Responsibility (OPR) will conduct the inherently governmental functions including the National Agency Check<sup>7</sup>, issue a Provisional Clearance and Final Suitability Determination, make all final polygraph determination, and conduct all quality assurance and quality control reviews. The CBP hiring process currently consists of a 12 step pre-employment process, along with the processing of new hires who have accepted a tentative job offer for employment. For example, the requirements for hiring Border Patrol Agents include:

- OPM Guidelines;<sup>8</sup>
- Border Patrol Agent Application Process;<sup>9</sup>
- CBP Suitability Overview;<sup>10</sup>
- Prior Drug-Use Guidelines;<sup>11</sup> and
- CBP follows best practices in its administration of the polygraph, which have been identified by the National Center for Credibility Assessment (NCCA).<sup>12</sup> All CBP polygraph examiners undergo the same NCCA training required of all federal polygraph examiners, and CBP's polygraph program has successfully passed five NCCA inspections.

---

<sup>7</sup> National Agency Check (NAC) is an integral part of all background investigations for federal employment. The NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary.

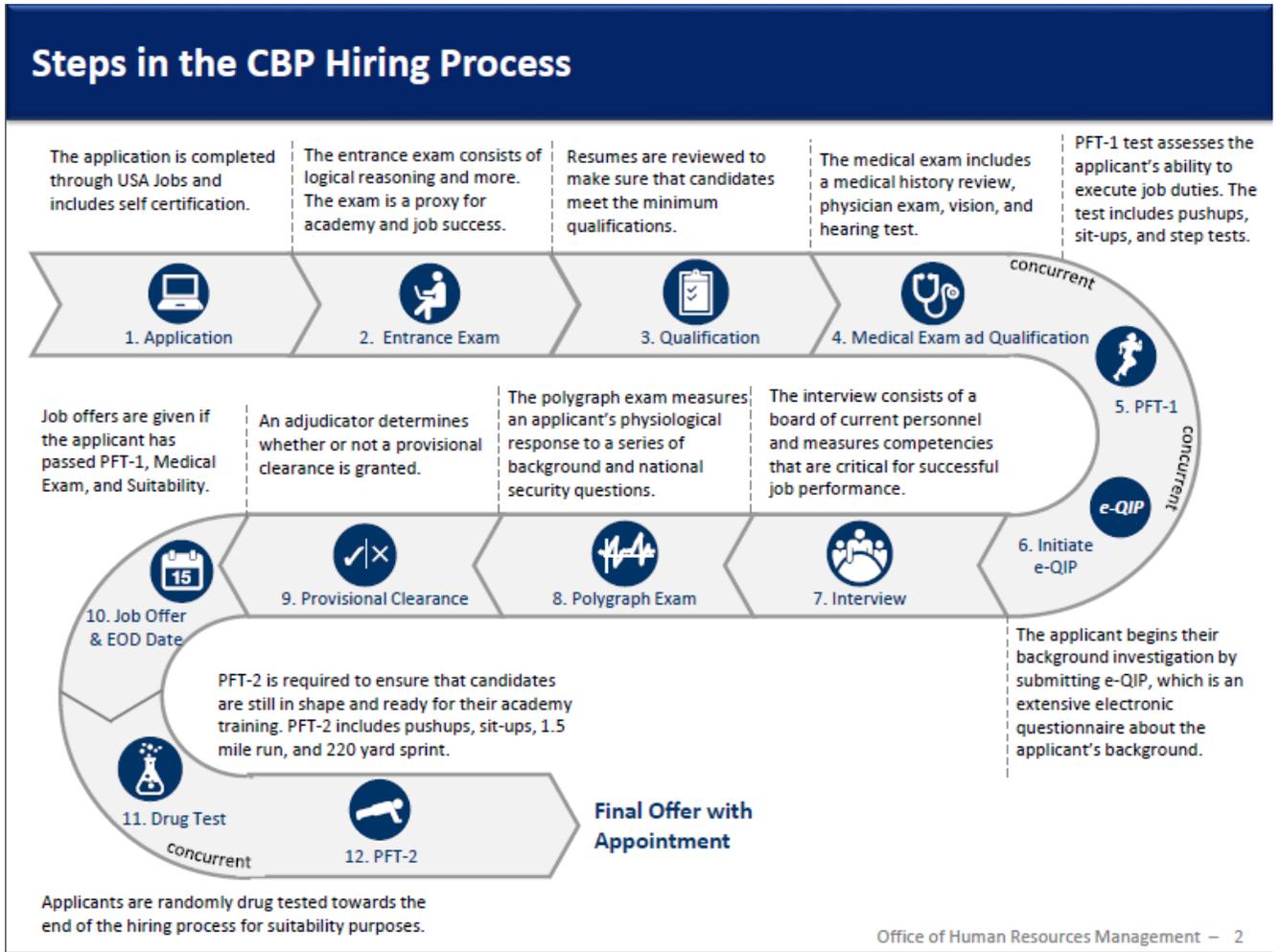
<sup>8</sup> OPM Classification Guidelines available at <https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/1800/border-patrol-enforcement-series-1896/>.

<sup>9</sup> See <https://www.cbp.gov/careers/frontline-careers/bpa/app-proc>.

<sup>10</sup> Applicants for law enforcement positions in U.S. Customs and Border Protection (CBP) are required to undergo a Tier V background investigation, previously known as a Single Scope Background Investigation (SSBI), and must submit to a polygraph examination as required by the Anti-Border Corruption Act of 2010. The results of the polygraph examination, in conjunction with information gathered as part of the background investigation process, is used to assess overall suitability and/or eligibility to hold a law enforcement position within CBP. Many of the questions asked during the polygraph examination and during the personal interview part of the background investigation will involve responses previously provided to questions on the application and background investigation forms. See <https://www.cbp.gov/careers/car/suitability>.

<sup>11</sup> CBP takes many considerations regarding previous illegal drug use into account in order to determine the suitability of an applicant. These considerations include, but are not limited to, frequency and recency of use, circumstances surrounding the use, the age of the person at time of use, contributing societal conditions, likelihood of recurrence, and/or a demonstrated intent to not use illegal drugs in the future. Regarding the recency of use, there is some use that will result in the applicant being found unsuitable. However, outside of this limited timeframe, recency of use will be just one factor that is considered when making a suitability determination about previous illegal drug use. See <https://www.cbp.gov/careers/car/prior-drug-use>.

<sup>12</sup> The National Center for Credibility Assessment (NCCA) is the federal center for credibility assessment education, oversight, research, and development. The Defense Intelligence Agency (DIA) operates control and oversight of the NCCA, which is based in Fort Jackson, South Carolina.



**Figure 1: Steps in the CBP Hiring Process for Frontline Positions**

### Parallel Recruiting and Hiring Functions

With the issuance of contract support for frontline hiring and recruiting services, CBP will essentially create two methods by which interested candidates can be recruited, apply for, and eventually be hired by CBP. Depending on how the individual was contacted or applied for a position with CBP, his or her information may be stored and used by AFS under the HRM 5000 program, or may be stored and used by CBP if collected under previous collection mechanism, such as via signing up for email alerts on [www.cbp.gov/careers](http://www.cbp.gov/careers).

AFS will employ targeted advertising and commercially available lists of potentially interested candidates based on research-driven target demographics. Due to these novel information collections, CBP is conducting this PIA to describe the HRM 5000 program, provide



transparency into the parallel hiring paths at CBP, and ensure that AFS is meeting federal statutory privacy compliance requirements, as well as DHS and CBP privacy policy requirements.

This PIA is drafted to broadly describe the technologies that AFS, on behalf of CBP, or CBP under its own human resources management programs, uses to collect, use, maintain, and share personally identifiable information. All information technology systems, tools, pilots, and tests will be included as an Appendix to this PIA, and will be regularly updated as HRM 5000 continues to expand. So long as AFS abides by applicable laws, regulations, and Agency policies, as well as the constraints noted above and listed in the published statement of objectives, they may use new and emerging technologies to recruit potential candidates for frontline positions. CBP will use this public-facing PIA to assess the privacy risk of and provide transparency about new technologies deployed by AFS and CBP. CBP will regularly update the Appendix of this PIA as HRM 5000 evolves.

AFS requires the ability to be nimble in its advertising and recruitment efforts; collect and maintain records on individuals who have voluntarily registered to receive marketing information related to CBP job opportunity announcements; manage communication with potential applicants or individuals who attend CBP career fairs or meetings in order to provide assistance during the CBP application process; and manage other recruiting and hiring activities.

## **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 derives the authority to collect the information in the National Frontline Recruitment and Hiring System from 5 U.S.C. § 302, Delegation of Authority; 44 U.S.C. § 3101, Records management by agency heads; Executive Order 13767, Border Security and Immigration Enforcement Improvements (January 25, 2017).

For suitability and personnel security functions, CBP relies on the following authorities: Executive Orders 10450, 12968, 13467, and 13488; 5 CFR § 731; 5 CFR § 732; 5 CFR § 736; 32 CFR § 147; Security Executive Agent Directive 5; and Director of Central Intelligence Directive 6/4.

The President's Transparency and Open Government Memorandum (January 21, 2009) and the OMB Director's Open Government Directive Memorandum (December 8, 2009) direct federal departments and agencies to harness new technologies to engage the public and serve as one of the primary authorities motivating CBP's efforts to use website data analytics.

Legal authorities and agency policies supporting CBP's use of third party website data analytics include:



- A. The President's *Memorandum on Transparency and Open Government*, January 21, 2009;
- B. The OMB Director's *Open Government Directive* Memorandum, December 8, 2009;
- C. OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010;<sup>13</sup>
- D. OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies*, and the Paperwork Reduction Act, April 7, 2010;<sup>14</sup>
- E. DHS Website Privacy Policy;<sup>15</sup>
- F. Google Terms of Service;<sup>16</sup>
- G. Google Privacy Policy;<sup>17</sup>
- H. Google Analytics Opt-out Browser Add-on;<sup>18</sup>
- I. Google Code of Conduct;<sup>19</sup> and
- J. Google Security and Product Safety.<sup>20</sup>

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

CBP considers AFS to be a “government contractor” pursuant to Section “m” of the Privacy Act of 1974, as amended,<sup>21</sup> which stipulates that, “when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.” This provision requires that AFS maintain all records collected on behalf of CBP and HRM 5000 to the same Agency requirements as CBP’s own collection, use,

---

<sup>13</sup> OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), available at [http://www.whitehouse.gov/omb/assets/memoranda\\_2010/m10-23.pdf](http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf).

<sup>14</sup> OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act* (April 7, 2010), available at [http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA\\_Gen\\_ICRs\\_5-28-2010.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRA_Gen_ICRs_5-28-2010.pdf).

<sup>15</sup> Available at [http://www.dhs.gov/xutil/gc\\_1157139158971.shtm](http://www.dhs.gov/xutil/gc_1157139158971.shtm).

<sup>16</sup> Available at <http://www.google.com/accounts/TOS>.

<sup>17</sup> Available at <http://www.google.com/intl/en/privacy.html>.

<sup>18</sup> Available at <http://tools.google.com/dlpage/gaoptout?hl=en>. (Available for Internet Explorer (versions 7 and 8), Google Chrome (4.x and higher) and Mozilla Firefox (3.5 and higher)).

<sup>19</sup> Available at <http://investor.google.com/corporate/code-of-conduct.html>.

<sup>20</sup> Available at <http://www.google.com/intl/en/corporate/security.html>.

<sup>21</sup> 5 U.S.C. § 552a(m) Government Contractors.



and maintenance of similar records. This provision also binds AFS' employees to the criminal penalty provisions of section "i" of the Privacy Act<sup>22</sup> for improper collection, maintenance, and dissemination of records covered by a Privacy Act system of records.

CBP collects frontline recruitment and hiring records pursuant to the newly issued DHS/CBP-025 National Frontline Recruitment and Hiring (NFRH) System of Records Notice (SORN).<sup>23</sup> This SORN provides notice of CBP's maintenance of records associated with CBP's recruitment and hiring efforts for frontline positions, and describes CBP's maintenance of records related to the recruitment and hiring of frontline CBP personnel. Per section "m" of the Privacy Act, this SORN covers records collected and maintained by AFS on behalf of CBP as part of the HRM 5000 initiative.

The SORN does not cover records associated with the traditional OPM hiring process once a potential applicant submits an application for employment. For these activities, the relevant OPM SORNs continue to apply.<sup>24</sup>

SORN coverage is not required for the use of website data analytics because the custom reports contain non-identifiable aggregated information, which is all that is provided to CBP. Google Analytics and other commercial website data aggregators are considered an external, third-party hosted, website(s) analytics solution.

The DHS/ALL-002 Mailing and Other Lists SORN also provides overall coverage for mailing lists maintained throughout DHS to facilitate mailings to multiple addressees and other activities in furtherance of CBP recruitment and hiring duties.<sup>25</sup>

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

No. HRM 5000 is not an IT system, but rather a program that will rely on existing CBP systems and contractor-owned systems consistent with the AFS procurement requirements. All CBP systems that are used by the HRM 5000 program are listed in the Appendix of this PIA.

---

<sup>22</sup> 5 U.S.C. § 552a(i)(1) Criminal penalties. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000. (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000. (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

<sup>23</sup> DHS/CBP-025 National Frontline Recruitment and Hiring System of Records, 83 FR 27014, (June 11, 2018).

<sup>24</sup> OPM/GOVT-5 Recruiting, Examining, and Placement Records, 71 FR 35351 (June 19, 2006).

<sup>25</sup> DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659, (Nov. 25, 2008).



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

The National Archives and Records Administration (NARA), General Records Schedule (GRS) 6.5, Item 20, and GRS 5.2, Item 20, governs the retention of recruiting and hiring records. CBP will delete records when superseded, obsolete, or when an individual submits a request to the agency to remove the records. In general and unless it receives a request for removal, CBP will maintain these records for 5 years, after which point they will be considered obsolete and no longer necessary for CBP operations.

## **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.**

CBP may obtain information about potential applicants either directly from the individual, from a third-party to whom the individual has granted permission to share his or her information with potential employers, or from community, civic, educational institutions, military, and other sources.

HRM 5000 must have an approved OMB information collection instrument for any collection of information.<sup>26</sup> Basic contact information solicited on the recruiting and marketing websites may not trigger the PRA provided that they entail no burden other than that necessary to identify the respondent, the date, the respondent's address, and the nature of the instrument (web form).

CBP has petitioned OMB under the "Generic Clearance for the Collection of Routine Customer Feedback" (OMB Control Number: 1651-0136) to collect survey information from potential CBP employees. Survey respondents will be self-selected by following a link to CBP's Microsite (<https://cbp.secure.force.com/applynow>). On the Microsite, they have the option to enter their first and last name, email address, telephone number, country (if not U.S.) and ZIP code, which will initiate follow up by a Recruiter. Adding additional survey information will enable applicants to provide additional information for the recruiter to gauge their general level of interest, current employment status, veteran status, and other details. This information will be stored with

---

<sup>26</sup> Collection of information means, except as provided in 5 CFR § 1320.4, "the obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit."



their personal information in a secure database, and used to assist potential applicants with the CBP hiring process and to improve their on-boarding experience.

Once a potential applicant has decided to formally begin the application and hiring process, the following OPM information collection requests apply:

- OMB No. 3206-0219 – USAJOBS 3.0.<sup>27</sup> The collection of information involves the use of the USAJOBS Resume Builder and Applicant Profile, which uses information technology and allows the upload of resumes and is fully web-based. This information is shared with the agency responsible for the Job Opportunity Announcement posting to begin the employment selection process.

For lists of potential applicants that CBP or AFS obtain from a third party, the PRA does not apply because CBP will not ask identical questions of ten (10) or more individuals. For the mass marking outreach communications to these individuals, they will always contain an opt-out feature that also does not trigger the PRA.

## **Section 2.0 Characterization of the Information**

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

CBP and AFS maintain information from individuals who have expressed interest in national frontline positions. This information includes:

- First and last name;
- Age or date of birth;
- Gender;
- Phone number(s);
- Email address(es);
- Mailing address(es), including ZIP code;
- Military status (e.g., veteran, active duty);
- Other biographic and contact information as required for hiring, recruitment, and outreach efforts;

---

<sup>27</sup> USAJOBS is the official one-stop collection point for Federal agency job postings and there are currently by law no other Government-wide collections such as this to facilitate hiring for all Federal Executive agencies.



- Various system-generated identifiers or case numbers;
- De-identified data related to analytics to measure the success of online marketing and advertising initiatives;
- Status of opt-in/consent to receive targeted marketing and advertising based on the individual's expressed area of interest in CBP employment opportunities; and
- Responses to pre-screening questions, including information related to: (1) an individual's possession of, or eligibility to, carry a valid driver's license (yes or no response only); (2) any reason why the individual may not be able to carry a firearm (yes or no response only); (3) interest level in CBP employment; (4) U.S. residency information (limited to length of residency only); and (5) any additional information in support of preliminary hiring activities.

CBP and AFS collect aggregated information on user interactions on CBP's website(s) such as number of visits, visitors, and type of browsers. CBP and AFS receive the non-identifiable aggregated information in the form of custom reports from third party website data analytics providers.

CBP and AFS collect applicant contact information from USAStaffing,<sup>28</sup> OPM's on-line recruitment and applicant management system that facilitates screening and hiring of employees for federal agencies. When an individual applies for critical CBP frontline law enforcement positions (i.e., U.S. Border Patrol Agents, Air and Marine Interdiction Agents, and CBP Officers) through USAStaffing, CBP and AFS receive the information in the form of custom reports from OPM.

CBP and AFS maintain the following information on individuals who have submitted applications to CBP via USAStaffing:

- Name;
- Social Security number (SSN);
- Contact information (telephone number(s), email address(es), and emergency contact);
- Position title, series, and grade;
- Written, oral, fitness, language, medical, drug test, and other applicable examination results;
- Current status in the hiring process; and
- Any information related to the background investigation process.

---

<sup>28</sup> See OPM/GOVT/PIA – USAStaffing (July 21, 2017), available at <https://www.opm.gov/information-management/privacy-policy/privacy-policy/usas-pia.pdf>.



CBP has published additional information related to CBP's collection and use of information on individuals in various stages in the relevant system PIAs, as listed in the appendix of this PIA.

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

HRM 5000 information is collected directly from individuals who express interest in jobs at CBP either at a job fair or recruitment event, through the CBP website or other sites sponsored by HRM 5000, through USAStaffing, or through third party job websites in which they have expressed an interest in employment with CBP or other law enforcement positions. In some instances, AFS may obtain information on prospective candidates from third parties with whom AFS partners in support of its hiring and recruitment initiatives, for example military, high school, or college career development centers. These candidates have generally expressed interest in employment opportunities similar to those offered by CBP, or are otherwise identified to be appropriate candidates for CBP recruitment initiatives.

As part of these relationships with third party hiring websites, AFS will deploy "resume mining" tools to search for candidates who may be interested in a career with CBP. All of these individuals will have consented to have their resumes searched by recruiters. Typically when a user creates (or uploads) a resume onto a third party hiring website, the user can choose a resume visibility status that determines who can view the resume. For example, most third party hiring websites permit the following options for recruiters to search resumes:

- Visible, where users and recruiters with access to the resume database will be able to view a user's contact information and resume, match the individual to specific jobs, and contact the individual directly.
- Limited, where users and recruiters with access to the resume database will be able to view the resume, match the individual to specific jobs, and contact the individual directly. However, they will not see potential applicant name, contact information, current employer, or references.
- Private, the individual resume will not be visible.

Visitors to these websites must consent and opt-in to include their resume in the third party website resume database. Typically these third party hiring websites include this information in their privacy policies. They also state that they post/upload an individual's resume as-is. So, for example, if an individual has included a Social Security number in his or her searchable resume, that would be searchable and available to AFS.



Individuals who visit AFS recruiting websites<sup>29</sup> may have their activities captured by commercial website data analytics. Third party website data analytics providers collect aggregated information from visitors to HRM 5000 websites using a combination of JavaScript<sup>30</sup> and first party cookies from the website domain. These sites are tagged with code containing a snippet of JavaScript that acts as a “beacon,” collecting non-personally identifiable visitor data (such as browser, operating system, referring page, and duration of page visit) and sending it back to the data collection servers for processing.

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

Yes. Aggregated data is obtained from Google Analytics, via HRM 5000 recruitment and hiring websites, and from third party hiring websites (e.g., Monster.com). All data pertaining to members of the public that is not provided directly by the individual is collected after the individual voluntarily registers to receive information from the CBP recruitment and hiring advertising campaign or other commercial recruitment websites that include CBP employment advertisements, or with whom AFS partners for hiring and recruitment activities.

### **2.4 Discuss how accuracy of the data is ensured.**

The majority of HRM 5000 information is collected directly and voluntarily from individuals who express interest in employment with CBP. Other information is sourced from OPM and CBP systems (for example, when an individual applies to a position with CBP through the USA Staffing process). HRM 5000 also gathers aggregate data analytics from website sources containing CBP employment advertisements. CBP’s website deploys capabilities allowing it to compare data analytics against historical website statistics, which allow it to identify any anomalies or trends that may indicate an error.

### **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** There is a privacy risk that DHS will collect and retain more information than is needed to identify and process viable applicants.

**Mitigation:** CBP mitigates this risk by ensuring that all information collected during the recruitment process is necessary to effectively and efficiently identify individuals that will qualify for frontline law enforcement positions. Though there is a risk of over collection, CBP limits the collection of PII to only the data that is necessary to the recruitment process.

---

<sup>29</sup> For example, the first public-facing AFS recruiting site is available at <https://cbp.secure.force.com/applynow/>.

<sup>30</sup> A scripting programming language most commonly used to add interactive features to websites.



**Privacy Risk:** There is a privacy risk that CBP will collect data analytics about browsing history or internet usage about beyond the scope of frontline recruiting and hiring.

**Mitigation:** This risk is mitigated. HRM 5000 does not use data analytics nor web tracking technologies to individually identify a user, nor track individual-level activity on the Internet. CBP's website deploys capabilities allowing it to compare data analytics against historical website statistics, which allow it to identify any anomalies or trends that may indicate an error. To minimize any possible privacy risk to visitors to the CBP public-facing website(s), CBP will not share data analytics with any third-parties. Individuals visiting the CBP public-facing website(s) will be able to opt-out completely. The CBP privacy policy provides information on how to opt-out of having cookies dropped in the visitor's browser. Visitors using a cookie blocker application will be able to visit the CBP public-facing website(s) and no information about their website experience will be processed by data analytics.

## Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

### 3.1 Describe how and why the project uses the information.

The HRM 5000 program goal is to conduct recruitment, marketing, outreach, and advertising to potential candidates for CBP frontline law enforcement positions. CBP and AFS will use information collected or obtained via HRM 5000 to generate leads and maintain lists of potential applicants for recruiting purposes based on commercially available demographic or subscription lists, or from community, civic, educational institutions, military, and other sources. CBP and AFS will identify quality candidates based on pre-screening question responses, manage all tracking and communications with potential candidates, and conduct outreach to retain applicants during the hiring process.

HRM 5000 allows CBP to notify individuals of new job opportunity announcements for which they may be interested. The CBP Hiring Center will maintain logs and respond to applicant questions from a national call center, and reengage applicants who withdraw from frontline hiring positions and invite them to reapply to CBP opportunities. CBP collects the individuals' biographic and contact information during the registration process when individuals express an interest in CBP employment information. The data collection activity takes place to identify candidates as leads, and to distribute targeted email and communication campaigns. Candidates must consent to the published privacy policy, opt-in to receive employment marketing advertisements via email, and to voluntarily self-identify for purposes of the DHS equal employment opportunity program; including the policies, practices, and procedures designed to ensure that all qualified individuals and potential applicants receive an equal opportunity for recruitment, selection, advancement, and any other term and privilege associated with CBP employment opportunities.



## Recruiting

Much of the initial information collected and maintained by CBP and AFS is in support of recruitment and advertising efforts aimed at increasing the number of individuals interested in a career with CBP. AFS will expand the diversity of CBP frontline applicants by targeting recruitment efforts both locally and nationally, and will use data analytics to drive CBP recruitment marketing and advertising strategy.

Through HRM 5000 recruitment, marketing, and hiring activities, CBP aims to (1) increase interest in employment with CBP; (2) expand and increase the diversity of the CBP applicant pool; and (3) improve efficiency and decrease overall time-to-hire. More broadly, HRM 5000 will identify best practices, process improvements, and efficiencies that will enable CBP to improve its recruitment and hiring activities over the long-term. The deployment of web analytics will allow CBP and AFS to assess, evaluate, and improve the performance of marketing and recruitment campaigns.

### *Use of Data Analytics*

Through the use of data analytics for recruitment and marketing, CBP and AFS will be able to measure the effectiveness of outreach campaigns involving both CBP websites, as well as various commercial recruitment and hiring websites. CBP will use aggregated information provided by Google Analytics<sup>31</sup> and other commercial website data aggregators in an effort to improve CBP recruitment and hiring services online. This will be done through the measurement and analysis of public-facing website traffic. Specifically, CBP will use non-identifiable aggregated information provided by Google Analytics, Google Tag Manager,<sup>32</sup> and pixels<sup>33</sup> placed within employment advertisements on CBP websites and other commercial employment websites to:

- track the number of visitors to CBP's public-facing website(s);
- collect aggregate recruitment source information to verify which CBP advertisements placed within CBP websites and various commercial recruitment websites collected the most activity; and
- understand the interactions of visitors in order to improve the functionality of the CBP's public-facing website(s) and the user experience by using the data analytics to focus future CBP advertisements placed on the web.

---

<sup>31</sup> Google Analytics is a web analytics service offered by Google that tracks and reports website traffic.

<sup>32</sup> Google Tag Manager is a tag management system created by Google to manage JavaScript and HTML tags used for tracking and analytics on websites. A tag is a keyword or term assigned to a piece of information that helps describe an item and allows it to be found again by browsing or searching.

<sup>33</sup> A tracking pixel is a pixel-sized image or graphic and short snippet of JavaScript loaded on a website when an individual visits a website and is used to track certain user activity.



However, to use commercial website data analytics, the product must collect the full IP Address<sup>34</sup> for analytical purposes, which Google and other providers will then mask prior to its use and storage, and proceed with providing CBP non-identifiable aggregated information in the form of custom reports.

For this initial phase of recruitment and marketing activities, CBP shall not collect, maintain, or retrieve PII, including a visitor's IP Address, during this analytics process. In the event that CBP and AFS deploy web tracking technologies, CBP will update this PIA to provide full transparency about the expansion of information collection.

For this phase, Google Analytics and other commercial data analytics providers shall not provide to CBP, share with a third party service or any product for additional analysis, or use the full or masked IP Address or associated information to draw any conclusions in the analytics product. The data analytics provider will receive the data to process and provide aggregate statistics back to CBP. The only information that is available is the non-identifying aggregated information in the data analytics interface in the form of custom reports that are only available to the CBP's public affairs officials, and senior leadership. Under **no** circumstances shall CBP use data analytics to:

- collect or track PII;
- collect or track a visitor's full or masked IP Address;
- track individual user-level activity on the Internet outside of CBP's website(s);
- cross-reference any data gathered from data analytics against PII to determine individual user-level online activity; or
- collect or track employees on CBP's internal facing web initiatives or products.

To the extent that the previously issued PIA for DHS's use of Google Analytics is applicable to new web tracking technologies, CBP will follow processes, procedures, and tracking methods for data analytics consistent with the DHS/ALL-033 PIA for the Department of Homeland Security Use of Google Analytics.<sup>35</sup>

### Independently post Vacancy Announcements

AFS uses information obtained from potential applicants as part of the recruitment and marketing efforts to direct them to AFS-created JOAs. AFS will determine whether applicants meet eligibility requirements based on their application responses. AFS will use the responses to pre-screen applicants who would not meet the basic hiring criteria by automated processes. These

---

<sup>34</sup> An IP Address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

<sup>35</sup> See DHS/ALL-033 PIA for the Department of Homeland Security Use of Google Analytics, *available at* <https://www.dhs.gov/privacy>.



determinations will be confirmed by manual review, in compliance with CBP HRM required procedures.

### Applicant Support/Care

In coordination with the recruitment efforts, AFS will use contact information to monitor candidate progress throughout the hiring process for both CBP stakeholders and applicants. This new information technology system will provide a snapshot of the number of eligible candidates for each major step in the hiring process, the current JOA status (open or closed), and the date(s) the last announcement(s) were open.

AFS has deployed several systems to meet this requirement including the Salesforce Platform and inContact, both detailed in the Appendix.

### Application Intake and Applicant Processing

AFS will use innovative and creative solutions to streamline the existing hiring process for frontline positions. Many of these functions or determinations are inherently governmental – for example the background investigation, polygraph determination, and suitability determination. However, AFS is exploring ways to, for example, improve or enhance the polygraph process and determine applicant eligibility. One way that AFS has expedited the eligibility process is by asking certain pre-screening questions prior to the formal application submission such as information related to: (1) an individual's possession of, or eligibility to, carry a valid driver's license (yes or no response only); (2) any reason why the individual may not be able to carry a firearm (yes or no response only); (3) interest level in CBP employment; (4) U.S. residency information (limited to length of residency only); and (5) any additional information in support of preliminary hiring activities.

As AFS deploys systems and functionality to modify or enhance the existing hiring and personnel security process, in particular as applied to the personnel security process, CBP will detail the systems and technologies in the PIA Appendix.

### **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. HRM 5000 does not use technology to locate a predictive pattern or anomaly.

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

Only CBP and AFS personnel have access to systems that support HRM 5000 hiring and recruitment activities. No other DHS Components have access to these systems or this information.



OPM personnel may access information from applicants, consistent with existing hiring procedures. A web portal allows members of the public to register online as potential applicants for CBP frontline positions; however, those individuals are only allowed to submit information and are not able to access any other parts of the system.

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a privacy risk that CBP will use the information it collects on members of the public for purposes other than recruitment and hiring, inconsistent with the original purpose of collection.

**Mitigation:** This risk is mitigated. During the recruitment phase, CBP and AFS only collect limited information from members of the public who voluntarily submit their information to CBP or another commercial employment-related website. CBP will not use this information for operational purposes (e.g., law enforcement), or for any other purpose that is not directly related to the original collection. CBP and AFS use information submitted during the hiring process consistent with previously published PIAs and SORNs; HRM 5000 and the partnership between CBP and AFS pose no change to the use of information obtained during the hiring process.

**Privacy Risk:** There is a privacy risk that CBP may use the information it collects in the system to disqualify an individual from CBP employment opportunities, inconsistent with the original purpose of collection.

**Mitigation:** CBP collects this information to help lead individuals to the correct CBP job announcement based on their expressed interest, and information volunteered by the individual during the registration process. Individuals may voluntarily self-identify in order to qualify for various equal employment opportunities within CBP.

## **Section 4.0 Notice**

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Individuals who provide their contact information via CBP or AFS webpages in order to obtain information about CBP employment opportunities are provided notice of CBP's collection of their information through Privacy Act statements. These statements articulate CBP's authority to collect the information, the purpose of the collection, the routine uses (or any sharing external to the Department), and any consequences related to the failure to provide the information. Third party websites that provide candidate information to CBP and AFS are required to advise the



individual that their information may be shared with potential employers, and candidates are required to opt-in to this sharing before their information is provided to a potential employer.

CBP provides notice of its collection of information in the National Frontline Recruitment and Hiring System of Records Notice,<sup>36</sup> published Privacy Act Statements on each AFS and CBP-owned recruiting site, and through the publication of this PIA.

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

Individuals who provide their information to CBP or AFS in order to receive information about CBP job opportunities do so voluntarily. Those who provide their information for this purpose may opt-out of additional communications via email communications from AFS. The same applies for individuals who have applied for positions with CBP, although these individuals must contact OPM to opt-out of certain notifications. Individuals who submit their information to third party websites (e.g., job search sites) or other partners who contract with AFS for employment purposes do so on a voluntary basis. Individuals whose information appear on recruiting lists that AFS purchases from recruiters, military, career counselors, or other commercial lists will have already provided consent to be contacted by those recruiters at the time they sign up for the original collection.

## **4.3 Privacy Impact Analysis: Related to Notice**

**Privacy Risk:** There is the risk that the individual may receive inadequate notice regarding the use of his or her information.

**Mitigation:** This risk is partially mitigated. CBP provides a Privacy Act Statement on the CBP websites; however, CBP does not read a Privacy Act Statement over the phone or in-person at CBP recruitment and hiring events. Providing an oral Privacy Act Statement is often impracticable in this environment. In such cases, CBP may direct individuals to a website, or provide a tear-sheet that includes a Privacy Act Statement. On HRM 5000 websites, individuals must confirm that they have read and understood the Privacy Act Statement before submitting their information. The Privacy Act Statement reminds individuals of the opportunity to decline to provide information, instructions to opt-out of tracking data analytics, and that the information is provided voluntarily.

---

<sup>36</sup> DHS/CBP-025 National Frontline Recruitment and Hiring Records, (June 11, 2018), 83 FR 27014.



## Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

In accordance with General Records Schedule (GRS) 6.5, Item 20, and GRS 5.2, Item 20, DHS/CBP will delete HRM 5000 records when superseded, obsolete, or when an individual submits a request to the agency to remove the records. In general and unless it receives a request for removal, CBP will maintain these records for 5 years, after which point they will be considered obsolete and no longer necessary for CBP operations. This is consistent with OPM guidelines for recruitment, examining and placement records,<sup>37</sup> which are retained for up to 5 years. For individuals who become CBP employees, certain records may be retained longer as part of the employee personnel file.

### 5.2 Privacy Impact Analysis: Related to Retention

There is no privacy risk to retention. CBP retains HRM 5000 records for the minimum amount of time necessary to conduct the HRM 5000 program goals of outreach, recruitment, and applicant care. For individuals who become CBP employees, CBP retains official personnel records consistent with the OPM SORNs.

## Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

### 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.

CBP and AFS do not routinely share HRM 5000 records outside of the agency. However, information may be shared externally in certain instances, in accordance with the routine uses outlined below.

As noted above, CBP considers AFS to be a “government contractor” pursuant to Section “m” of the Privacy Act of 1974, as amended, which stipulates that, “when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.” This provision requires that AFS maintain all records collected on behalf of CBP and HRM 5000 to the same Agency requirements as CBP’s own

---

<sup>37</sup> OPM/GOVT-5 Recruiting, Examining, and Placement Records (June 19, 2006), 71 FR 35351.



collection, use, and maintenance of similar records. This provision also binds AFS and its employees to the criminal penalty provisions of section “i” of the Privacy Act for improper collection, maintenance, and dissemination of records covered by a Privacy Act system of records.

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

CBP does not intend to share the HRM 5000 records outside of the CBP enterprise, including with AFS and AFS-subcontractors. However, in the event that CBP may share HRM 5000 records external to the Agency, CBP will share records in accordance with the NFRH SORN and pursuant to the published routine uses including:

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS’s efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. 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.

These uses are compatible with the original purpose of the SORN because they (1) ensure compliance with Federal policy related to incident and breach response (routine uses E and F); (2) enable sharing of information that is of critical relevance to assessing an individual’s integrity and



suitability for employment with CBP (routine use G); and (3) are necessary in order to fulfill the recruitment and hiring mandates for which this initiative was created (routine use H).

### **6.3 Does the project place limitations on re-dissemination?**

Yes. CBP places limits on the re-dissemination of information shared with other federal agencies, including through the use of a Memorandum of Agreement (MOA) or a letter of authorization. These documents contain provisions that ensure compliance with the Privacy Act, and authorize disclosure via the routine uses contained within the SORN. AFS, like all contractors or service providers that receive or handle CBP information, must comply with the same limitations on re-dissemination and protections.

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

CBP tracks any sharing of HRM 5000 records using the DHS Form 191, Privacy Act Disclosure Record, and retains a copy of these forms and the underlying request for a period of five years.

### **6.5 Privacy Impact Analysis: Related to Information Sharing**

**Privacy Risk:** There is a privacy risk that CBP may improperly disclose HRM 5000 information outside of the agency, or to someone without a verified need-to-know.

**Mitigation:** This risk is mitigated. CBP and AFS ensure that all individuals accessing HRM 5000 information are trained on the appropriate procedures for sharing information outside of CBP. All information is shared on a case-by-case basis only as authorized by law, and CBP advises the recipient that the information may not be re-disseminated without CBP's express prior approval.

## **Section 7.0 Redress**

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals may verify and update their information 1) through a telephone call to CBP National Hiring Centers at 1-833-405-8051; and 2) by requesting access to the information contained in the National Frontline Recruitment and Hiring Records made to CBP's FOIA Office via FOIA online at <https://foia.cbp.gov/palMain.aspx>, 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

All Privacy Act and FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

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

Since members of the public and other federal agency personnel do not have direct access to the HRM 5000 records, they must request assistance from CBP to view and correct their individual records. Individuals may request correction by calling the CBP National Hiring Centers or through a Privacy Act or FOIA request, as described above. CBP and AFS will take all appropriate steps to verify the requestor's identity and ensure the information requires correction prior to modifying the record.

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

During the registration process for individuals to obtain information regarding CBP frontline positions, the individuals are prompted to confirm their information and are given the opportunity to correct their information at that time. In addition, Privacy Act Statements refer individuals to the NFRH SORN, which describes access and correction procedures for all HRM 5000 records.

## **7.4 Privacy Impact Analysis: Related to Redress**

There is no privacy risk related to redress. All information is submitted directly by the individuals. CBP provides substantial notice via the public-facing website(s) and Privacy Act Statements. If individuals are not satisfied with their ability to update their information, they may contact the CBP National Hiring Center for assistance, or they may file a Privacy Act Request.



## Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

In order to minimize or mitigate the risk of unnecessary or inappropriate use of information, CBP and AFS use the following controls in administering systems that contain HRM 5000 information:

- Database access must be requested through a supervisor;
- User names are assigned by the system;
- Access is role-based and determined by user profile;
- Only users with an official need-to-know, designated by the system administrator, will be able to access sensitive information once an individual is registered;
- Actions within the system are tracked automatically by the system via the Audit Trail Report; and
- All HRM 5000 contractors are required to have a fully adjudicated background investigation prior to onboarding and accessing any CBP systems or data.

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

All system users must complete both an annual privacy and information technology security-related training, as well as other training required by the contract.

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

CBP and AFS systems control data access through data partitioning of domains and user roles. A domain defines the data a user can access; the role establishes what the user can do with that record in the database. Domain access and user roles are configured in the system according to the business requirements set forth by the Standard Operating Procedure. Access to the system falls in two general categories: (1) administrative users (*e.g.*, recruiting coordinators, recruiting managers, hiring center staff); and (2) system administrators including database administrators and network engineers.



The system administrator grants access to administrative users at the request of the user's supervisor or contracting officer's representative. The request must specify the level of access required and verify the user's need-to-know. If approved, a profile is created and a role is assigned to the user.

## **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?**

Long-standing procedures govern access to, or sharing, of information from CBP systems. Information sharing agreements/arrangements are drafted by the CBP Office of Human Resources Management in consultation with the Office of Information Technology program managers. Arrangements that involve PII are sent to the CBP Privacy Officer for review and to DHS for final approval in accordance with procedures developed by the DHS Information Sharing Governance Board.

### **Responsible Officials**

Suzanne Shepherd  
Program Manager  
HRM 5000/Enterprise Services  
U.S. Customs and Border Protection

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

### **Approval Signature**

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

---

Philip S. Kaplan  
Chief Privacy Officer  
Department of Homeland Security



## Appendix A: Technologies, Tools, and Systems Used by HRM 5000

The HRM 5000 Program will evolve as the marketing and outreach needs are assessed and fine-tuned by AFS and CBP. This Appendix provides a comprehensive overview of the technologies, systems, and tools that AFS on behalf of CBP, or CBP on its own, are using to advance the HRM 5000 Frontline hiring and recruiting mission.

CBP will continually update this Appendix during the HRM 5000 deployment.

### **1. Salesforce Platform (July 11, 2018)**

CBP provides frontline recruitment and hiring services through a Customer Relationship Manager Tool that uses a cloud service provider called the Salesforce platform. The Salesforce Recruitment Application is currently composed of distinct recruiting and hiring functions as follows:

- **Lead Management:** The CBP website(s) allow individuals to voluntarily join the CBP Talent Network, and lead candidates to available job opportunity announcements. Individuals who provide contact information (name, email, phone, and mailing address) agree to allow CBP to engage and communicate with the individuals in the future. The ability to track and manage activities that occur with the individual, such as receiving communication via phone or email, confirmation of selecting opt-out from receiving future communications, and identify if the individual has applied for a position.
- **Lead Engagement:** The ability to ask individuals prescreening questions or assist individuals with answering questions and documenting the details in their individual record. Additionally, the individuals will be engaged with communications and notifications about CBP frontline career opportunities and upcoming events, and receive encouragement to apply for positions CBP will also manage any outreach activities to organizations, associations, identified partners, or educational institutions who would be a key demographic to market CBP frontline positions to. The activities associated with the outreach will be documented in the system.

### **2. inContact (July 11, 2018)**

The CBP National Hiring Centers utilize inContact, a fully integrated cloud contact center system. inContact provides the capability to manage telephone call queues online and the ability to electronically distribute calls among CBP employees located at the CBP National Hiring Centers concerning the various phases within the recruitment and hiring process. To comply with the CBP's enterprise data model, the contact center staff shall document the nature of each call by notating the issue, resolution, or escalation in the form of a case status for the incoming caller.



### 3. Human Resource Business Engine (HRBE) (July 11, 2018)

The activity managed by the CBP National Hiring Centers is recorded in the Human Resources Business Engine's (HRBE) Customer Inquiry Tracking workflow with respect to tracking and inquiry management where cases are created when CBP receives communications from individuals either over the phone or email regarding the hiring process. HRBE Entry Level Hiring (HRBE-E) collects applicant personal information including name, Social Security number (SSN), date of birth, address, phone, and email, which are obtained from USA Staffing as part of the application process. This data is used in various parts of the hiring process including pre-employment testing as well as for general communications with applicants. The process to collect records associated with a potential applicant who submits an application for employment is governed under the DHS/CBP-032 PIA for the HRBE system.<sup>38</sup>

### 4. Salesforce Marketing Cloud (December 7, 2018)

CBP uses the Salesforce Marketing Cloud in support of its digital marketing campaign. This digital marketing automation and analytics software enables mass email functionality through the development of email templates; automation and on-demand emailing; management of the customer life-cycle; and use of a custom email domain to be used with the Salesforce Marketing Cloud that enables all emails to be sent from a designated masked IP address. Individuals sign up for CBP's email marketing campaign via the CBP Salesforce Recruitment Application and the Salesforce Marketing Cloud maintains only the email address and subscriber status. If an individual unsubscribes from a specific email list, the Salesforce Marketing Cloud logic automatically populates the subscriber status field with an unsubscribed value, thereby disabling all future email campaigns for the email address. The email addresses of unsubscribed individuals are then deleted from the system. The Salesforce Marketing Cloud manages both automated and manual email campaigns to disseminate information pertaining to the recruitment and hiring process.

CBP accepts the security risk for use of the Salesforce Marketing Cloud. The Salesforce Marketing Cloud is not yet FedRAMP certified; however, CBP will amend the existing security authorization for the CBP Salesforce platform to include the Marketing Cloud. Because the Salesforce Marketing Cloud has not yet achieved FedRAMP certification, CBP has limited the amount of PII within the system to only include an email address for individuals who voluntarily sign up to receive email marketing campaigns.

### 5. HRM Frontline Hiring Dashboard (May 6, 2020)

---

<sup>38</sup> See DHS/CBP/PIA-032 Human Resources Business Engine (HRBE), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



CBP uses the HRM Frontline Hiring Dashboard, a Microsoft Power Business Intelligence (Power BI) tool located in the Microsoft Azure Government Cloud that is used to display aggregate information for each phase of the hiring process in order to showcase real-time national frontline hiring and onboarding data. The dashboard provides a snapshot view of hiring data to allow CBP to analyze business process requirements for recruiting, onboarding lifecycle, retention, and resources, to determine if there are any bottlenecks in the hiring process that can be addressed, and to understand how CBP can use the information to ensure success in each business process.

The hiring process overview displays aggregate level data for all cases in process to confirm the total number of applicants moving through each stage of the hiring process and includes a filter to display the applicant source, as well as the type of position applied for. The dashboard is configured for role-based access such that only users that have an “authorized need to know” can view additional screens.

The dashboard is populated with information that applicants have previously provided to CBP throughout the hiring process. CBP retains this information in multiple source systems, such as the CBP Credibility Assessment and Polygraph Service (CAPS),<sup>39</sup> HRBE, the DHS Integrated Security Management System (ISMS),<sup>40</sup> and the USA Staffing system. The data sources are used to display the status of each stage within the hiring process. While the information displayed in the dashboard is aggregated, the Applicant ID and Person ID are exported from HRBE. This data is visible on some screens to allow users to track the progress of individuals throughout the hiring process. The dashboard does not include any other PII, such as the name, SSN or date of birth.

The type of data that populates the dashboard includes: applicant position, active duty status, process age (i.e., average length of time an individual spends in each stage of the hiring process), location, Electronic Questionnaire for Investigation Processing (e-QIP) status, structured interview status, medical exam status, fitness test status, drug test status, background investigation status, and polygraph exam status.

---

<sup>39</sup> A PIA for CAPS is in progress at the time of publication of this appendix entry.

<sup>40</sup> See DHS/ALL/PIA-038 Integrated Security Management System (ISMS), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).