Privacy Impact Assessment
for the

Hiring Information Tracking System (HITS)

May 13, 2010

Contact Point
Robert Parsons
Director, Office of Human Capital
U.S. Immigration and Customs Enforcement
(202) 732-7770

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Hiring Information Tracking System (HITS) is an information system used by U.S. Immigration and Customs Enforcement (ICE) to track current and prior hiring actions. HITS maintains information about individuals who are selected for vacant positions at ICE. ICE has conducted this Privacy Impact Assessment (PIA) because HITS collect personally identifiable information (PII) about individuals who are offered employment with ICE.

Overview

HITS is owned by the ICE Office of Human Capital (OHC). The purpose of HITS is to create a record for and track the hiring of ICE personnel as they progress through the various stages of the hiring process. HITS tracks the ICE job vacancy from the time it is created until a new hire enters-on-duty at ICE to fill the vacant position. HITS data includes position information, vacancy announcement information, and information on the person selected to fill the vacant position (“selectee”). HITS contains data that is automatically updated through electronic interfaces with other information systems. Other HITS data is entered manually by ICE Hiring Center personnel in Laguna Nigel, California. In order to track the hiring process, HITS interfaces with or obtains information from the following information systems, which are discussed below: Table of Organization Position System (TOPS), USAJOBS, Electronic System for Personnel (ESP), Customs Applicant Pre-Employment System (CAPES) and Security Analysis and Reporting System (SARS).

HITS and the ICE Hiring Process

The ICE hiring process begins when an ICE program office identifies a need to hire for a vacant position. The hiring office first initiates a recruitment action within ICE’s ESP using the government’s Standard Form 52 (SF-52). ESP creates a recruitment action that is automatically transmitted to HITS, which then creates a master hire record and triggers another ICE system, known as the Table of Organization Position System (TOPS), to automatically send additional information about the vacant position to HITS. TOPS sends the following position data to HITS: position number, organization code, hiring program, employee type, position title, grade, pay plan, and job code. The data transmitted to HITS from ESP and TOPS does not contain any PII.

Once the ICE hiring office has received approval to hire for a vacant position, it works with OHC to prepare and finalize the vacancy announcement for the vacant position. ICE uses the U.S. Office of Personnel Management’s (OPM) USA Staffing system to announce and solicit applicants for ICE job vacancies. Once ICE posts the vacancy announcement with USA Staffing, it is displayed in USAJOBS and individuals may apply for vacant ICE positions by submitting a resume and completing ICE’s Online Application Questionnaire using USAJOBS’s Application Manager. Once a vacancy announcement is closed or reaches an established cut-off date, ICE Hiring Center personnel use USA Staffing to review the qualified applicants’ information and identify eligible candidates using applicable criteria for the particular job vacancy. In USA Staffing, ICE Hiring Center personnel prepare a “selection certification” containing the list of qualified candidates and refer it to the ICE official that will make the final candidate selection ("selecting official"). The ICE Hiring Center personnel then enter the announcement dates and selection certificate information (certificate number, issue date, date selection made, and grade of selectee) into HITS.

After the selecting official makes a selection from among the candidates, he or she notes which candidate was selected on the selection certificate and returns it to the ICE Hiring Center. ICE Hiring Center personnel manually enter the selectee information in HITS and notifies the selectee of the offer. If the selectee accepts, they are then assigned a projected enter-on-duty date, which is entered into HITS, and the hiring office logs into ESP to complete the SF52. Selectees are processed through some or all of ICE's five hiring tracks which are prerequisites for the vacant position: Oral Boards, Fitness, Drug Test, Medical, and Security. Not all of the five tracks are required for all selectees for all positions. Which tracks are required depend on factors such as whether the selectee is currently an ICE employee, holds an active security clearance, or if the position requires a higher level of fitness proficiency than the one in which the selectee is certified.

As the selectee progresses through the Oral Boards, Fitness and Medical tracks, ICE Hiring Center personnel update HITS manually with the results/outcomes of those tests. For the Drug Test track, ICE Hiring Center personnel manually enter in HITS the date the drug test was requested by ICE. HITS receives the drug test results date through an automated daily interface with the U.S. Customs and Border Protection system called the CAPES which stores limited information about the results, specifically whether the candidate cleared (i.e., passed) the test, did not clear, or cancelled. The actual results of drug tests are not stored in HITS, although HITS does contain a notation to indicate whether the candidate cleared (i.e., passed) the test. For the Security track, HITS receives data about the selectee through an automated interface with ICE's SARS Security data received by HITS includes the dates the personnel security forms were sent to and received from the selectee; the date fingerprint cards were received by ICE personnel; and the dates the selectee's personnel security investigation was initiated and completed. In the future, SARS will be replaced by the DHS system called ISMS (Integrated Security Management System), which will provide the same data to HITS through an automated interface.

After successfully completing all applicable tracks, the selectee is assigned a scheduled enter-on-duty date. After the selectee enters on duty, ICE Hiring Center personnel update HITS to reflect that the hiring action for the position vacancy is completed. The Hiring Center updates the master hire record in HITS with the actual enter-on-duty date for the selectee. If the selectee does not enter on duty for any reason (e.g., they do not successfully complete one of the hiring tracks, or they decide to take another job instead), all of the selectee information except for the name of the individual is deleted from the record and the reason is annotated in the comments section of the record.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

HITS maintains information about individuals who are ultimately chosen by selecting officials at ICE for vacant positions, and who accept the offer of employment and report for duty. HITS also maintains data on selectees that declined the position or did not complete the hiring tracks successfully. For these persons, all PII except name is deleted from the HITS record when it becomes clear they will not be reporting for duty in the vacant position.

- HITS maintains the following types of information about selectees:
  - Selectee name, Social Security number, date selected, and selection grade (General Schedule level).
- HITS maintains information about the various tracks selectees must complete as a prerequisite to being hired for the vacant position.
  - For the Oral Boards track, HITS data includes the scheduled date of the oral board interview and the whether the selectee passed or failed.
  - For the Fitness and Medical tracks, HITS data includes the initiation date, follow-up date (if necessary), and the dates the selectee successfully completed each of the two tracks.
  - For the Drug Test track, HITS data includes the date the drug test was requested and completed, if they are cleared (i.e., if they passed). Actual results of drug tests are not stored in HITS, only whether they are cleared.
  - For the Security track, HITS data includes the dates the security forms were sent to and received from the selectee; the date the fingerprint cards were received by ICE; the date the personnel security investigation was initiated and cleared.

1.2 What are the sources of the information in the system?

ICE obtains most selectee information directly from the selectee's application for employment for the ICE vacancy. Drug testing information is provided through a data extract from CBP's CAPES. Dates relating to the Security track are provided to HITS through an interface with ICE's SARS.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected and maintained to allow ICE to efficiently track the progress of its hiring actions and to ensure that persons selected for vacant positions are suitable for those jobs by successfully completing evaluations and training that are prerequisites for those positions. Hiring data may also be used for trend analysis.

1.4 How is the information collected?

ICE collects the selectee's information directly from the selectee during the application process using the USAJOBS application software. The selectee provides responses to the application questionnaire and submits their resumes to ICE via the USAJOBS website. ICE Hiring Center personnel manually enter selectee information into HITS from USA Staffing once the selection certificate has been returned from the selecting official. Information regarding the selectee's personnel security investigation is automatically provided to HITS via an automated interface with SARS. Drug testing dates are entered manually by ICE Hiring Center personnel, but the drug testing completion dates are provided to HITS via a data extract from CBP's CAPES.

1.5 How will the information be checked for accuracy?

ICE verifies the information provided by the selectee by verifying it against the identification documents presented by the selectee and through a background investigation. Other information is verified manually from forms submitted from the applicant and information received from the various hiring tracks.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Authority is provided by the Homeland Security Act of 2002, which authorizes DHS to issue regulations with regard to employment of individuals in the Federal Service and maintain their records. 5 U.S.C § 9701, et seq., provides authority for the establishment of a human resources management system.

DHS Management Directive 121-01, establishes the Office of the Chief Security Officer of DHS, and the DHS Instruction Handbook 121-01-007, The Department of Homeland Security Personnel Suitability and Security Program, June, 2009, establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a privacy risk that personally identifiable information recorded within HITS may be transmitted via unsecure methods.

Mitigation: The risk has been mitigated by ICE's transmitting data from other systems through secure electronic transmission.

Privacy Risk: There is a privacy risk that unauthorized users may gain access to the system.

Mitigation: The risk is mitigated by granting access to the physical database software to individuals that have a need to know. Access to the data software components is administered through the COTS Security software package. This software is also used to ensure password generation compliance, verify attempted access, and reject unauthorized attempts for access.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

HITS information is used to track the selectee's progress through the hiring process. The selectee must fulfill the hiring conditions of the position before being assigned a date to enter-on-duty. The dates recorded for the hiring tracks indicate the selectee's completion of tracks in the hiring process. The selectee's Social Security number and name is used to identify the individual applying for employment with ICE and distinguish the selectee from others with similar names. It is also used during the personnel security checks to help verify employment, education, and other key elements of the background investigation. HITS data is also used by ICE to determine hiring process timelines and trends.

2.2 What types of tools are used to analyze data and what type of data may be produced?

HITS can run simple reports to identify vacancies by district and title within hiring control offices; vacancies by projected scheduled and actual enter-on-duty dates; and vacancies that have not yet been funded. HITS reports also include vacant positions with selectee information; selectee status; vacancy and selection process tracking; vacancies by hiring and security status. In addition, there are reports by hiring status staffing levels; vacancy announcement; applicant and statistical reports.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

HITS does not use or contain commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The security package used by ICE to administer access to its mainframe systems ensures that only authorized personnel with a need to know are granted access to this system's software and data components. In addition, users of these systems complete ICE's mandatory annual privacy and security training, which stresses the importance of authorized use of personal data in government systems.

Section 3.0 Retention

3.1 What information is retained?

All information entered into HITS is retained in the system. This includes data identified in Section 1.1 of this document as well as data relating to Vacancy Announcements, Personnel Recruitment Actions and Positions and the hiring process tracks as well as training scheduling.

3.2 How long is information retained?

ICE proposes that the selectee data on individuals that actually enter-on-duty be retained for five (5) years after notification of death or the employee separation date from ICE. These records will be retained for this period to provide ICE OHC with management reporting and trend analysis capabilities. Other than the selectee's name, data on selectees who do not enter-on-duty will be removed from HITS within 30 days from the time notification is received that the employee will not enter on duty.

ICE will retain HITS user audit logs until ICE determines they are no longer needed for administrative, legal, audit, or other operational purposes. This retention period is necessary to help system administrators facilitate the reconstruction of events if compromise or malfunction occurs or is suspected.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. ICE has drafted a retention schedule for the information retained in HITS and NARA approval is pending. The retention schedule will include the proposed retention periods described in Question 3.2 above.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: The risk presented is that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The information in HITS is retained for the timeframes outlined in Question 3.2 to ensure selectee information is available to ICE for an appropriate period to facilitate the hiring process of ICE employees. This retention period is generally consistent with the retention of human resources data and appropriate in length given the need to use the data for trend analysis and administrative purposes in support of the ICE mission. In addition, data on selectee's that will not enter on duty is deleted within 30 days of receiving this notification.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

ICE does not share HITS data with any other DHS component. HITS is used exclusively by hiring center personnel. HITS data is not transmitted outside of ICE. This information is maintained in the Electronic Official Personnel Folder (eOPF) of the individual. Any sharing of information will come directly from eOPF rather than HITS.

4.2 How is the information transmitted or disclosed?

ICE does not share or transmit this data with any other DHS component. This data is not transmitted outside of ICE. This information is maintained in the Electronic Official Personnel Folder (eOPF) of the individual. Any sharing of information will come directly from eOPF rather than HITS.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

This information is not shared outside of ICE.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ICE does not share this data with external organizations. This data is not transmitted or shared outside of ICE. This information is maintained in the Electronic Official Personnel Folder (eOPF) of the individual. Any sharing of information will come directly from eOPF rather than HITS.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The General Personnel Records SORN (OPM/GOVT-1, June 19, 2006, 71 FR 35356) and the Recruiting, Examining, and Placement Records SORN (OPM/GOVT-5, June 19, 2006, 71 FR 35351) provide notice regarding the collection and maintenance of this information.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

ICE does not share this data with external organizations. This data is not transmitted to or shared outside of ICE. This information is maintained in the Electronic Official Personnel Folder (eOPF) of the individual. Any sharing of information will come directly from eOPF rather than HITS.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

This information is not shared outside of ICE.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

Yes. The applicants are provided the notice at the time they are completing the application for employment. The OPM application provides a Privacy Act Statement that informs the applicant of the authority and purpose of the collection, the possible ways the information will be shared and whether providing the information is voluntary or mandatory. The OPM/GOVT-1 SORN regarding civilian personnel records and OPM/GOVT-5 SORN pertaining to the recruitment, examining and placement records provide notice regarding the collection and maintenance of this information.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, but if an applicant elects not to provide this information, he or she may not be eligible for ICE employment.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. If the applicant provides the information on the application, there is no opportunity to consent to some uses and not others. Each use of information will comport with the OPM/GOVT-1 General Personnel Records, and OPM/GOVT-5 Recruiting, Examining, and Placement Records SORNs.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: There is a risk of a lack of notice of the collection and uses of the information.

Mitigation: Individuals who seek to apply for employment with ICE are provided four forms of notice: this PIA, the General Personnel Records SORN; the Recruiting, Examining, and Placement Records SORN; and the Privacy Act Statement included on the employment application. Notices are accurate and reflect the current stated uses and sharing of the information. This notice is sufficient to mitigate any risks associated with a lack of notice of the collection of the information or the uses of the information.

Section 7.0 Access, Redress and Correction

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

Applicants are provided with a copy of their application at the time of submitting the application form. Individuals seeking notification of and access to any record contained in HITS, or seeking to contest its content, may submit a request to the ICE FOIA Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information on how to submit a FOIA. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals seeking notification of and access to any record contained in HITS, or seeking to contest its content, may submit a request in writing to the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website (http://www.ice.gov/foia) for additional information on how to submit a FOIA. Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. If an individual believes more than one DHS component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: A risk is presented that individuals are not aware of their ability to make record access requests for records in HITS.

Mitigation: This risk is mitigated by the publication of this PIA, the OPM General Personnel Records SORN, and the OPM Recruiting, Examining, and Placement Records SORN, which describe how individuals can make access requests under FOIA or the Privacy Act.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

To request access to HITS, users complete the Password Issuance and Control System (PICS)[1] Form G-872A and forward it to the responsible information technology official. These requests are then

[1] *See* PICS PIA at www.dhs.gov/privacy.

forwarded to a PICS Security Officer for processing. The supervisor must supply the type of access the user needs (update access or view only) within HITS. Access to data within HITS is controlled at the organization level by assigning an organizational code pertaining to the specific field or Headquarters offices that the human resources employee is servicing. Listed below are the user roles for HITS:

- **System Administrators:** System administrators have the highest level of access. They are responsible for the maintenance of HITS and are responsible for user access controls.
- **Update Access:** These users are responsible for updating information within HITS. All users with update access are able to update master hire data for any hire action for positions within their authorized organization code list.
- **View Only Access:** These users have the lowest level of access and may only view the data within their authorized organization code list.

8.2 Will Department contractors have access to the system?

Yes. System access is granted to DHS contractors performing hiring related activities within the ICE Hiring Centers and ICE program offices. All contractors must request access through the procedures described in Question 8.1.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Training for HITS is conducted by OHC personnel or by OHC-authorized contractors. Training is available for users new to HITS or those requiring refresher training. HITS instructor-led classroom training includes guidance on appropriate uses of the system and data. A training guide for these sessions is provided to attendees.

In addition, all ICE personnel and contractors complete annual mandatory privacy training called “A Culture of Privacy Awareness.” This course provides information to enhance general awareness of how to protect the personal information entrusted to an employee of DHS. This training expands the learner's knowledge of general privacy concepts and introduces the essentials of compliance with the Privacy Act of 1974 and E-Government Act of 2002. This training helps DHS employees and contractors to recognize situations in which privacy issues arise and how best to mitigate risks to privacy in the development and operation of a program.

Employees and contractors are also required to take annual mandatory training called Information Assurance Awareness Training (IAAT). The new name reflects the true scope of the course--maintaining the confidentiality, integrity, and availability of information of all types. This course provides information on the following: protecting computers from malicious software; protecting information systems from unauthorized access; maintaining the confidentiality of sensitive information, including personally identifiable information (PII); recognizing and avoiding security threats at home and while traveling; and recognizing and reporting a security or privacy incident.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. HITS was granted an Authority to Operate (ATO) on January 16, 2007. The ATO expired on January 16, 2010, however, a new ATO is anticipated in April 2010.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

HITS verifies user credentials with each attempted access to the HITS database to ensure the user has the appropriate access to the data requested. The type of access is also verified with every activity. The HITS application specific audit trail captures information associated with any insertion, update, or deletion of records in the database. This information will include the date/time of the activity, identification of the user that performed the activity and the values changed during the activity. The HITS application audit trail provides adequately detailed information to facilitate the reconstruction of the events prior to the time of system compromise or malfunction. The ICE database level audit trail provides information pertaining to logon attempts (successful and unsuccessful) and data viewing. All audit trails are protected from actions such as unauthorized access, modification and destruction. HITS audit records are stored within HITS at the time of hire record modification and will be retained as described in the forthcoming HITS record retention schedule.

ICE has a process in place for investigating and responding to suspicious activities regarding the system. That process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. HITS runs within the DHS network and is protected by DHS network firewalls. The real time interfaces to HITS are between HITS and other ICE applications protected by DHS firewalls.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: The privacy risks associated with this system are primarily the risks of unauthorized system access and inadequate system security.

Mitigation: Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion interdiction software, and user training. Mainframe and desktop computer access is behind locked doors, with card reader and/or guard access controls.

Section 9.0 Technology

9.1 What type of project is the program or system?

HITS is a mainframe application internal to ICE that supports hiring of ICE personnel.

9.2 What stage of development is the system in and what project development lifecycle was used?

This project is in the Operations & Maintenance (O&M) stage and was developed using the governance documents in force by the government at the time of its development in 1996, Immigration and Naturalization Service (INS) System Development Life Cycle (SDLC) v 4.0.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement

Approval Signature

____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security