Privacy Impact Assessment
for the

DHS Enterprise e-Recruitment System

March 3, 2008

Contact Point
Monica Doyle
Office of the Chief Human Capital Officer
Center for Talent Management and Accountability
(202) 357-8244

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS), Office of the Chief Human Capital Officer (OCHCO) is implementing an enterprise e-Recruitment system for DHS. The use of an automated recruitment solution is necessary to meet mission critical needs of DHS and comply with the 45-day hiring model under the President's Management Agenda. OCHCO has conducted this privacy impact assessment (PIA) because e-Recruitment will use and maintain personally identifiable information.

Introduction

The Department of Homeland Security (DHS), Office of the Chief Human Capital Officer (OCHCO) is implementing an enterprise e-Recruitment system for DHS. The use of an automated recruitment solution is necessary to meet mission critical needs of DHS and comply with the 45-day hiring model under the President's Management Agenda.

Technology-enabled recruitment can deliver both time savings and improved results. Based on an internal inventory of DHS human resource (HR) systems, more than 50 systems are currently used by DHS components to perform hiring/recruitment related activities. As part of the effort to consolidate and modernize the HR systems, the OCHCO is leading an effort to consolidate towards an automated enterprise solution that can contribute to material improvements in the overall hiring process.

Working in close collaboration, OCHCO's Human Capital Business System (HCBS) and Human Capital units defined the key project goals. The overall vision for the e-Recruitment initiative is to implement a state-of-the-art system that automates hiring/recruitment processes across DHS and seamlessly integrates with other related DHS services. Key high level goals for this system are:

- Automate the processes used to manage the full recruitment/hiring life cycle
- Create a single portal for all job applicants
- Provide a flexible solution that is adaptable to the needs of individual DHS components
- Reduce manual processes and/or eliminate paper paper-based systems
- Provide an easy to use interface for applicants, personnel specialists, and managers
- Implement industry best practices
- Reduce hiring/recruitment costs

It is envisioned that the e-Recruitment solution will provide automation to support six major functions of the hiring/recruitment cycle: (1) workforce planning; (2) requisitioning; (3) candidate talent searching; (4) candidate acquisition; (5) applicant tracking and (6) reporting & analytics. OCHCO led a collaborative effort within DHS to collect and prioritize the full range of business requirements and system functionality that will be needed by all organizational components.

Architecture and Interface

e-Recruitment will rest behind the primary federal hiring and recruitment website, www.usajobs.gov. In some instances a candidate will go directly to the e-Recruitment web interface by going to www.dhs.gov /careers, but initially the majority of traffic will be through the usajobs.gov website. Once a user has selected a job to apply for on the usajobs.gov website, they will be directed, after proper notice, to the e-Recruitment website. Once on the e-Recruitment website, the user will be required to create a username and password and complete a user profile much like the usajobs.gov site (see Section 1.1 regarding user profile data elements) This information will be stored in the e-Recruitment database and will be usable for any job the user may apply for at DHS.

If an individual is hired, e-Recruitment will interface with the DHS personnel system and the payroll system maintained for DHS at the US Department of Agriculture (USDA) National Finance Center in order to send the new employee's information to that system. Only post-hire employee information will be sent to other DHS systems.

Typical Transaction

A potential applicant will find a listing for a DHS job on the usajobs.gov website and choose to apply for the position. After clicking "apply now" on the usajobs.gov website, the applicant will be given and must accept a notice that he is leaving usajobs.gov and then will be taken to the DHS e-Recruitment domain and will be voluntarily entering personally identifiable information (PII) into a DHS system. After completing the aforementioned user profile (see Architecture and Interface section, above), the applicant will complete the rest of the application for employment, to include responding to job related evaluation criteria concerning qualifications and competencies, education and training, and general employment criteria such as U.S. citizenship and veteran preference.

Once completing the application itself, e-Recruitment will help OCHCO employees manage the evaluation and hiring process of the individual. E-Recruitment will help OCHCO manage the minimum qualification determination assessment of the application, certification of the application (whether an applicant is one of the more qualified candidates), interview, reference checks, tentative and final offers, and security checks (security checks and clearance procedures are conducted in conjunction with the DHS Office of Security processes).

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The e-Recruitment system collects information spanning the hiring/recruitment life cycle. This will include information on individual job applicants' names, addresses, job skills, and work history. Additionally, the system will track applicants as they proceed through the hiring process, capturing interview notes, assessment tests, and candidate scoring.

In general, all records in this system contain identifying information including name, date of birth, Social Security number, and home address. The SSN and Date of Birth will be collected from applicants who are selected for jobs. Date of birth will be collected from applicants who have applied for jobs that are covered by maximum entry age requirements.

These records pertain to the determining eligibility for employment and to the assessment of applicants' qualifications for the positions which they apply. The records contain information on both competitive examinations and on certain noncompetitive actions, such as determinations of time-in-grade restriction waivers, waiver of qualification requirement determinations, and variations in regulatory requirements in individual cases.

This system includes records described in and covered by the following Office of Personnel Management (OPM) government-wide (OPM/GOVT) systems of records: OPM/GOVT-5, Recruiting, Examining, and Placement Records, and OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records. These systems of records notices were last published in the Federal Register at 71 Fed. Reg. 35,341-35,363 (June 19, 2006). For workforce planning activities performed in e-Recruitment, employee data may be derived from the Office of Personnel Management Government-wide systems of records: OPM/GOVT-1 General Personnel Records which is also published in the Federal Register at 71 Fed. Reg. 35,341 (June 19, 2006).

To view data elements see Attachment A.

1.2 From whom is information collected?

Information will be collected from individual applicants either directly or via third party assessment services or recruiting systems (e.g., USAJOBS). DHS HR specialists and hiring managers will also enter information into the system relating to the applicant evaluation and selection processes.

1.3 Why is the information being collected?

Information will be collected and processed for two fundamental reasons: (1) maximize the size and quality of candidate pools for positions at all levels of DHS, and (2) provide selecting officials with the best-qualified candidates in minimal time.

The records are used to consider applicants for positions at DHS by making determinations of qualifications, including any medical qualifications required for the position, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates to DHS components for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. Records derived from the OPM-developed or DHS-developed assessment center exercises may be used to determine training needs of participants. These records may also be used to locate applicants and employees for personnel research (such as conducting statistical surveys) as well as to disclose information to federal agencies in response to investigative requests and judicial or administrative proceedings in accordance with the Privacy Act and the routine uses established in the governing systems of records notices identified above in Section 1.1.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The Homeland Security Act of 2002 called for the establishment of a new human resources system for the DHS that is flexible and contemporary. In related legislation, the E-Government Act of 2002 called for the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation. It also called for the adoption

of innovative information technology, including the appropriate use of commercial best practices. Authority for Maintenance of the System: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

1.5 Privacy Impact Analysis

Application inflow to DHS exceeds two million resumes/applications annually. In 2004, DHS filled over 28,000 positions. In view of the amount and type of data being collected, OCHCO unauthorized system access poses the greatest privacy risk to the confidentiality of the data collected and stored by the e-Recruitment system. As described in Section 8 of this PIA, DHS OCHCO has taken significant steps to mitigate those privacy risks.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Based on research conducted by HCBS that included consultation with a leading information technology research and advisory company, Internet searches, literature searches and live demonstrations of e-recruitment systems, many best practices were identified for each aspect of the recruitment process. The hiring/recruitment information collected will enable DHS to implement best practices for creating and using prescreening questions on a DHS-wide level to reduce manual processes, providing an easy-to-use interface for all system users, reduce hiring costs, and create a single portal for applicants. The information will be used to: plan recruitment efforts based on workforce analytics regarding turnover rates and expected budget/FTE allocations; proactively recruit for anticipated vacancies to reduce the time-to-hire; automate employee referrals, applications, pre-screening, resume management, candidate tracking, and candidate rating and ranking; provide applicant workflow, communications, interview management, reference/background checking, and "on-boarding" services; provide regulatory and analytical reports for both recruiters and hiring managers.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

The e-Recruitment system will have the capability to perform reporting/analytics that enable DHS to project vacancies and determine best sources for candidates. The system will also provide dashboards to display key metrics and reports/tracking.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Access to the e-Recruitment system will be role-based so that only authorized system users can view, enter and update information. Additionally, information is collected directly from an applicant and generally entered by the applicant or DHS personnel. The system will minimize the opportunity for providing inaccurate responses by using specific drop down lists and data fields with formats that constrain responses according to pre-defined rules. During the applicant evaluation process, authorized DHS staff and hiring managers will be responsible for validating information provided by applicants, to the greatest extent possible by comparing information provided by the applicant in response to job related evaluation criteria

and general eligibility questions to the documentation submitted by the applicant (e.g., resume, veteran preference eligibility, career transition assistance program eligibility, Federal employment status) to supplement and support their application for a specific job.

2.4 Privacy Impact Analysis

Given the amount and type of information collected, robust auditing functions are built into the system to provide an audit trail sufficient to reconstruct security relevant events and regularly reviewed to prevent unauthorized activity. Additionally, by utilizing role-based access, the system will be able to create, maintain, and protect information from unauthorized modification, access, or destruction.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Applicant records will be maintained for a maximum time period of two years in accordance with the General Records Schedule 1 (GRS 1) as discussed in section 3.2 below.

See attachment B for retention periods for specific records as extracted from GRS 1.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. The e-Recruitment system will comply with the National Archives Records Administration (NARA) Retention Schedule for civilian personnel records relating to recruitment. Merit Promotion and Delegated Examining Unit (DEU) cases are retained mainly for the purpose of appeals from applicants who were not selected and/or not found qualified. There are numerous categories for hiring-related files with varying retention periods under the General Records Schedule, Transmittal No. 15, September 2005. Two years is the maximum time period for retention of any such records.

3.3 Privacy Impact Analysis

The purpose of retaining the information is to provide DHS the capability to re-construct the hiring/recruitment/selection process and address any hiring-related issues or complaints that may arise after selections are made. The data will also be used to respond to any Equal Employment Opportunity (EEO) issues or law suits. Retaining these records in accordance with GRS 1 will help to mitigate attendant privacy risks associated with maintaining these records.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The e-Recruitment system is an enterprise-wide implementation, information may be shared with DHS organizational components based on a specific need to identify, evaluate, and process applicants to their respective components. The DHS Equal Employment Opportunity (EEO) and Civil Rights/Civil Liberties

offices will be granted access to all hiring/recruitment data to enable them to assess compliance with federal and DHS employment objectives and reporting requirements.

4.2 For each organization, what information is shared and for what purpose?

As each DHS organizational component has its own delegated hiring authority, the system will provide the component's human capital office with shared access to applicant information for the purpose of enabling the component's human capital office staff members to perform their respective hiring/recruitment activities in an efficient manner. As an enterprise system, e-Recruitment will provide a single platform for use by all DHS components. Normally, data will not be shared between components but hiring metrics will be aggregated for departmental reporting purposes. For example, applications for similar positions may be exchanged between components, but all analytical reports such as those described in Section 2.1 will be reported based on an aggregate basis with no reference to specific individuals. When data is shared, it will be for a specific need for the component to access applicant files to identify, evaluate and process applicants (for example, surge hiring that occurs to respond to a disaster) to meet a particular hiring need. The DHS EEO and Civil Rights/Civil Liberties offices will be granted access to all hiring/recruitment data and related demographics to enable them to assess compliance with federal and DHS employment objectives.

4.3 How is the information transmitted or disclosed?

e-Recruitment is accessed through a commercial hosting provider under contract to DHS and the system will comply with appropriate security requirements and procedures under the Federal Information Security Management Act (FISMA), applicable federal law, and policy for the e-Recruitment system. The system includes several layers of security to ensure that only authorized users can access information stored in the system. Secure Sockets Layer (SSL 3.0) software will be used to encrypt all data transmissions back and forth between the hosting data center and the end user's web browser.

4.4 Privacy Impact Analysis

Given the enterprise nature of the system, internal organizational components will utilize the system and/or possibly share applicant information. Role-based security will limit internal sharing of data. For instance, applicants will only be able to view their personal records, selecting supervisors will be able to view all of the applications for their vacant position, and HR specialists will have access to all records in the system for the organizations that they service.

Records are maintained in a secured environment with access limited to authorized DHS personnel and contractors whose duties require access.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Generally, organizations external to DHS will be not allowed to access information related to DHS applicants whether the information is directly entered into, or otherwise captured by, the e-Recruitment system. However, OPM and the Government Accountability Office (GAO) may gain access to the information as part of an authorized audit. Information may also be shared in accordance with the provisions of the Privacy Act and the applicable routine uses identified in the applicable system of records notices identified in Sections 1.1 and 6.1.

5.2 What information is shared and for what purpose?

See response to 5.1 above.

5.3 How is the information transmitted or disclosed?

Information would be transmitted in a secure fashion to meet the needs of the audit.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

No. See response to 5.1 above.

5.5 How is the shared information secured by the recipient?

Any Federal agency receiving this information is required to handle it in accordance with the Privacy Act, the Federal Information Security Management Act (FISMA), and their applicable Privacy Act system of records notices.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No specific training is required by DHS in order to access the information in the system. Federal agency employees and their contractors typically are required to undergo Privacy Act training by their employing agencies.

5.7 Privacy Impact Analysis

Information in the system will be shared in accordance with the Privacy Act and the routine uses in the applicable Privacy Act system of records notices. Generally, information in the system will be shared within DHS for official purposes only so DHS anticipates sharing information with OPM and GAO pursuant

to an audit. These limits will effectively reduce attendant privacy risks.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Yes. As described in Section 1.1, the following OPM government-wide system of records notices apply to the information in the e-Recruitment system:

OPM/GOVT-1, General Personnel Records, 71 Fed. Reg. 35, 341 (June 19, 2006). *Description*: Current and former Federal employees as defined in 5 U.S.C. 2105.
(Volunteers, grantees, and contract employees on whom the agency maintains records may also be covered by this system).

OPM/GOVT-5, Recruiting, Examining, and Placement Records, 71 Fed. Reg. 35,341, 35,351 (June 19, 2006) *Description:* Records on (a) persons who have applied to OPM or agencies for Federal employment, and current and former Federal employees submitting applications for other positions in the Federal Service; and (b) applicants for Federal employment believed or found to be unsuitable for employment on medical grounds.

OPM GOVT-7, Applicant Race, Sex, National Origin and Disability Status Records, 71 Fed. Reg. 35, 341, 35,356 (June 19, 2006) Description: Records on current and former Federal employees and individuals who have applied for Federal employment used by OPM and agencies to evaluate personnel/organizational measurement and selection records, implement and evaluate Federal Equal Opportunity Recruitment and affirmative action programs, prepare reports regarding breakdowns by race, sex, and national origin of applicants, and to locate individuals for personnel research. In addition, a Privacy Act Statement will be provided to inform applicants of the purpose for collecting the information, the authority to collect the information, the routine uses of such information, and whether provision of the information is voluntary or mandatory.

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

Yes, submission of resumes and supporting information is voluntary and users will be notified that they have the right to decline to provide this information. Also, the system allows candidates to accept or decline job offer to include reason(s) for declination via e-mail or letter.
The collection of unsolicited resumes is standard practice over the internet and Application Service Providers (ASPs) that support recruitment services. HCBS' intention is to leverage the current OPM standard via USAJOBS model. USAJOBS/OPM has completed a separate PIA and OPM provides a privacy

statement to applicants regarding the collection of personal information. If an applicant posts their resume on the internet via a recruitment site (public, private sector or personal web pages) the information is in the public domain. With the applicant's permission, his/her application may be referred to the selecting official for specific vacancies. We anticipate that this practice will be limited to "hard-to-fill" positions for which qualified, available, interested candidates are scarce.

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

See response to 6.1 above. The routine uses of the information are defined in the applicable system of records notices. In addition, the Privacy Act Statement will inform applicants regarding their rights to particular uses of information. Some data collected (e.g., RNO) will be expressly identified as "voluntary".

6.4 Privacy Impact Analysis

Information in the e-Recruitment system comes from the individuals to whom it applies or is derived from information the individual supplied, reports from medical personnel on physical qualifications, results of examinations that are made known to applicants, agencies, and OPM, and references or other sources that the applicant lists or that are developed. All information is submitted by the applicants on a voluntary basis and adequate notice is provided via the application, which provides applicants with a Privacy Act Statement.

Section 7.0 Individual Access, Redress and Correction

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

The use of user IDs and passwords will allow applicants to gain access to their own resumes and/or any supporting documentation that may be provided.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." 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.In accordance with the DHS Privacy Act Regulation at 5 C.F.R. §5.21(d), individuals making a Privacy Act request with DHS or a DHS component must provide the following information:

a. Full name
b. Current address
c. Date of birth
d. Place of birth
e. Sign the request pursuant to penalty of perjury (28 U.S.C. §1746) or have the signature notarized.

In order to help DHS identify your records more easily, you may wish to provide the following additional information:

a. Social Security number (if provided).
b. Identification number (if known).
c. Approximate date of record.
d. Title of examination or announcement with which concerned.
e. Geographic area in which consideration was requested.

Individuals requesting access to OPM records under the Privacy Act must comply with OPM's Privacy Act regulations on verification of identity and access to records (5 CFR Part 297).

7.2 What are the procedures for correcting erroneous information?

Applicants and DHS system users (i.e., Human Resource specialists and hiring managers) will be able to modify erroneous information subject to the proper use of user ID and password access controls. The system allow applicants to create, update, view and monitor activities on their profile. The system will prompt applicants to electronically certify their application or re-application upon completion or modification. The system records and stores all certification dates and allow the HR users to enter certification dates for paper applications.

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

Applicants will be provided instructions and hyperlinked guidance to assist them with making corrections to their information. System users will receive formal training on the e-Recruitment system and have user guides to which they can reference. Additionally, help desk support will be available to assist system users. Further, individuals may request correction of their records in accordance with the DHS Privacy Act regulation at 5 C.F.R. §5.26.

7.4 If no redress is provided, are alternatives are available?

Redress is provided through Privacy Act access, correction, and redress.

7.5 Privacy Impact Analysis

Given the access and other procedural rights provided for in the Privacy Act of 1974, job applicants may direct any privacy-related concerns to OCHCO or file a Privacy Act request. Any such requests for correction and/or redress will be expeditiously addressed.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

System users will be HR specialists and hiring managers within DHS. Furthermore, applicants will have access to the system over the Internet via a web browser using encryption and secure access protocols.

8.2 Will contractors to DHS have access to the system?

The e-Recruitment system is hosted by an approved DHS commercial Application Service Provider (ASP). Therefore, a limited number of contractors would have access to the system based on a need to maintain or use the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the system will be role based to segregate users' access to data and functionality.

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

The system will accommodate different levels of user access, providing secure access to menus and data that is appropriate to different user needs. Procedures will be developed, documented and implemented to establish access controls.

Designated System Administrators will control user access to DHS sensitive information based on positive user identification and authentication mechanisms. Access control measures employed within the system will provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. System Administrators will ensure personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. In addition, they will divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The e-Recruitment system uses rules and roles based approach to establish and grant access to authorized users to instill segregation of duties. The e-Recruitment system provides audit-tracking reports for user access, usage logs, and e-Recruitment data structures. The audit trails will identify and list each access, the device accessing or attempting to access the system, the time and date of access and logoff time. Audit logs are periodically reviewed to ensure the system has been accessed by authorized personnel and in accordance with their level of access.

The e-Recruitment system includes several layers of security to ensure that only authorized users can access information stored in the application. Secure Sockets Layer (SSL) software is used to encrypt all transmissions back and forth between the hosting data center and the end user's web browser.

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

The e-Recruitment system will provide summarized and detailed reports on user access, usage logs, and key e-Recruitment data structures in order to monitor system usage and prevent misuse of data. The audit trail will include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. Audit logs will be periodically reviewed to ensure that only authorized users are granted access in accordance with their prescribed role and to ensure that audit trails are protected from modification, unauthorized access, or destruction and are retained and regularly backed up. These audit records will not be physically deleted or altered, except as part of a system administration archival process and will be restored as necessary. The audit data shall be protected so that read-only access to it is limited to those who are authorized.

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

All DHS employees and contractors are required to take mandatory Security Training prior to accessing a federal system. This security training course includes an overview on Privacy and Personally Identifiable Information (PII).

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

As with other OCHCO enterprise systems, the Certification and Accreditation (C&A) documentation for e-Recruitment is currently under development. At the completion of the C&A the system will comply with FISMA requirements. The DHS Risk Management System Application will be used to create, maintain and update the C&A for the System.

The system enables applicants to view, print, or sends a read-only version of their application after a vacancy announcement has closed. The applicants will be able to save their application package to their local drive. The system shall automatically notify the HR user of any changes to the application package.

Currently, application and system administration support users remotely access the e-Recruitment system via a secure VPN with two-factor authentication. System users, including external applicants, helpdesk personnel, DHS managers, and off-site HR service providers (contractors) will initially access the system using the web unique identifier, via SSL 128-bit encryption. Application users will use the IE browser and web interface with HTTPS to access the system.

The C&A for the system will be approved prior to the system going operational.

8.9 Privacy Impact Analysis

Privacy risks are mitigated by the enforcement of access controls within the system to establish segregation of duties. Consequently, access is established based on the user's job role. Access to the data in turn is assigned to correspond with the job function and the user's area of responsibility. Audit trails are maintained and reviewed regularly to ensure that no unauthorized access or misuse of the system occurs. Collectively, these procedures will help to prevent unauthorized access to the system.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system is a commercial off the shelf (COTS)-based solution that leverages existing technologies in the market place.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The data privacy and security aspects of the e-Recruitment system were defined by a departmental working group in consultation with the Special Security Officer assigned to Human Capital. Each proposal was evaluated against its ability to satisfy the DHS data integrity, privacy and security requirements.

Furthermore as part of the C&A process, e-Recruitment has been subjected to a comprehensive assessment of the technical, operational and management security controls to determine its compliance. As part of the C&A process, the DHS Information System Security Officers (ISSO) will conduct a review of the system and site surveys to ensure it is operating in accordance with security requirements.

9.3 What design choices were made to enhance privacy?

Required system features were identified based on extensive market research conducted by OCHCO staff. The market place for e-Recruitment vendors is crowded and many of the solutions have similar implementations (same basic features but some variations in user interfaces). The primary design choice centered on self-hosting versus using a commercial ASP. Based on previous experience with other enterprise software, a commercial ASP is a viable approach and can be implemented quickly.

Conclusion

Automating the hiring/recruiting function in DHS will provide broad benefits. It will encourage people to apply for positions at DHS by creating a more positive experience for applicants, significantly reduce hiring time, eliminate most manual steps in the process, and reduce costs by replacing many stove piped systems within DHS with a single enterprise-wide system. This system will reduce the broader security risks posed

to DHS by continued use of numerous individual systems and/or manual processes spread throughout the department. Although consolidating all hiring/recruitment functions is not without risk, such as those as described above, the solution will employ state of the art security features such as those inherent in other HCBS sponsored enterprise systems that are already being deployed.

Responsible Officials

John S. Allen, Human Capital Business Systems

Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Attachment A

Data Elements

Page		
Personal Information	**Personal Information**	First Name
		Last Name
		Middle Name
		Street Address (Line 1)
		Street Address (Line 2)
		City
		Zip/Postal Code
		Country
		State/Province
		Nearest City
		Email Address
		Primary Number: Home Phone; Work Phone
		Email Address
	Source Tracking	Source Type
Experience	**Work Experience**	Current Job
		Employer
		Employer Street Address
		Employer City/Town
		Employer State/Province
		Employer Country
		Start Date
		End Date
		Formal Title
		Salary
		Average hours per week
		May we contact your supervisor
		Series
		Grade/Band/Level
		Duties, Accomplishments and Related Skills
		Job Related Training
	Education	Education Level
		Institution
		Major
		Country
		State/Province
		Nearest City
		Total credits earned
		Graduation date
		System for awarded credits
	Certification/Licenses	Certification/License
		Issuing Organization
		Issue date

Page	Section	Field
Citizenship Questions	**Citizenship Questions**	Are you a US Citizen? If you are not a US Citizen, please provide the country of your citizenship

Attachment B

e-Recruitment Electronic Files covered by

GENERAL RECORDS SCHEDULE 1

Civilian Personnel Records

Agency civilian personnel records relate to the supervision over and management of Federal civilian employees. This schedule covers the disposition of Official Personnel Folders of civilian employees and other records relating to civilian personnel. The following e-Recruitment records are covered by GRS1;

Official Personnel Folders (OPFs).

Records filed on the right side of the OPF. (See GRS 1, item 10, for temporary papers on the left side of the OPF). Folders covering employment terminated after December 31, 1920, excluding those selected by NARA for permanent retention.

a. Transferred employees.

See Chapter 7 of *The Guide to Personnel Recordkeeping* for instructions relating to folders of employees transferred to another agency.

b. Separated employees.

Transfer folder to National Personnel Records Center (NPRC), St. Louis, MO, 30 days after latest separation. [See note (2) after this item]. NPRC will destroy 65 years after separation from Federal service.

[**NOTES**: (1) OPFs covering periods of employment terminated prior to January 1, 1921, are not covered by this item. If an agency has such files, it should contact NARA to request appraisal of the files. If NARA rejects the records, the disposition for GRS 1, item 1b applies. (2) Certain agencies have been exempted by OPM from retiring their OPFs to NPRC. These agencies retain OPFs for the period specified in item 1b of this schedule and effect destruction after that period has elapsed.]

2. Offers of Employment Files.

Correspondence, including letters and telegrams, offering appointments to potential employees.

a. Accepted offers.

Destroy when appointment is effective.

b. Declined offers:

(1) When name is received from certificate of eligibles.

Return to OPM with reply and application.

Temporary or excepted appointment.

File with application (see GRS 1, items 33k, 33l, 33m, or 33n, as appropriate).

All others.

Destroy immediately.

3. Certificate of Eligible's Files.

Copies obtained from OPM of certificates of eligible's with related requests, forms, correspondence, and statement of reasons for passing over a preference eligible and selecting a non-preference eligible.

Destroy when 2 years old.

4. Position Classification Files.

Position Classification Standards Files.

Standards and guidelines issued or reviewed by OPM and used to classify and evaluate positions within the agency.

Destroy when superseded or obsolete.

(2) Standards and guidelines issued or reviewed by OPM and used to classify and evaluate positions within the agency.

Correspondence and other records relating to the development of standards for classification of positions peculiar to the agency, and OPM approval or disapproval.

Case file.

Destroy 5 years after position is abolished or description is superseded.

(b) Review File.

Destroy when 2 years old.

b. Position Descriptions.

Record copy of position descriptions that include information on title, series, grade, duties and responsibilities, and related documents.

Destroy 2 years after position is abolished or description is superseded.

5. Interview Records.

Correspondence, reports, and other records relating to interviews with employees. Destroy 6 months after transfer or separation of employee.

Equal Employment Opportunity (EEO) Records.

a. Official Discrimination Complaint Case Files.

Originating agency's file containing complaints with related correspondence, reports, exhibits, withdrawal notices, copies of decisions, records of hearings and meetings, and other records as described in 29 CFR 1613.222. Cases resolved within the agency, by Equal Employment Opportunity Commission, or by a U.S. Court.

Destroy 4 years after resolution of case.

b. Copies of Complaint Case Files.

Duplicate case files or documents pertaining to case files retained in Official Discrimination Complaint Case Files.

Destroy 1 year after resolution of case.

c. Preliminary and Background Files.

(1) Background records not filed in the Official Discrimination Complaint Case Files.

Destroy 2 years after final resolution of case.

(2) Records documenting complaints that do not develop into Official Discrimination Complaint Cases.

Destroy when 2 years old.

d. Compliance Records.

(1) Compliance Review Files.

Reviews, background documents, and correspondence relating to contractor employment practices.

Destroy when 7 years old.

(2) EEO Compliance Reports.

Destroy when 3 years old.

e. Employee Housing Requests.

Forms requesting agency assistance in housing matters, such as rental or purchase.

Destroy when 1 year old.

f. Employment Statistics Files. [See note after this item.]

Employment statistics relating to race and sex.

Destroy when 5 years old.

7. Merit Promotion Case Files.

Records relating to the promotion of an individual that document qualification standards, evaluation methods, selection procedures, and evaluations of candidates.

Destroy after OPM audit or 2 years after the personnel action is completed, whichever is sooner.

8. Examining and Certification Records.

Delegated agreements and related records created under the authority of 5 U.S.C. 1104 between the OPM and agencies, allowing for the examination and certification of applicants for employment.

a. Delegated agreements.

Destroy 3 years after termination of agreement.

b. Correspondence concerning applications, certification of eligibles, and all other examining and recruiting operations. Such correspondence, includes, but is not limited to, correspondence from Congress, White House, and the general public, and correspondence regarding accommodations for holding examinations and shipment of test materials.

Cut off annually. Destroy 1 year after cutoff.

c. Correspondence or notices received from eligibles indicating a change in name, address, or availability.

Destroy 90 days after updating the appropriate record in the registry or inventory.

d. Test material stock control.

Stock control records of examination test material including running inventory of test material in stock.

Destroy when test is superseded or obsolete.

e. Application Record Card (OPM Form 5000A, or equivalent).

Cut off after examination. Destroy no later than 90 days after cutoff.

f. Examination Announcement Case Documentation Files.

Correspondence regarding examination requirements, final version of announcement(s) issued, subsequent amendments to announcement(s), public notice documentation, rating schedule, job analysis documentation, record of selective and quality rating factors, rating procedures, transmutation tables, and other documents associated with the job announcement(s) and the development of the register/inventory or case examination.

Cut off after termination of related register or inventory or after final action is taken on the certificate generated by case examining procedures. Destroy 2 years after cut off.

g. Register or inventory of eligibles (OPM Form 5001-C or equivalent, documenting eligibility of an individual for Federal jobs).

Destroy 2 years after the date on which the register of inventory is terminated.

h. Letters to applicants denying transfer of eligibility (OPM Form 4896 or equivalent).

Cut off annually. Destroy 1 year after cutoff.

i. Test Answer Sheets.

Written test answer sheets for both eligibles and ineligibles. Filed by date of processing.

Destroy when 6 months old.

j. Lost or Exposed Test Material Case Files.

Records showing the circumstances of loss, nature of the recovery action, and corrective action required.

Cut off files annually. Destroy 5 years after cutoff.

k. Cancelled and ineligible applications for positions filled from a register or inventory. Such documents include Optional form (OF) 612, resumes, supplemental forms, and attachments, whether in hard copy or electronic format.

Cut off annually. Destroy 1 year after cutoff.

l. Eligible applications for positions filled from a register or inventory, including OF 612, resumes, supplemental forms, and attachments, whether in hard copy or electronic format.

(1) On active register or inventory.

Destroy 90 days after termination of the register or inventory, (except for those applications that may be brought forward to a new register or inventory, if any).

(2) On inactive register or inventory.

Cut off annually. Destroy 1 year after cut off.

m. Ineligible or incomplete applications for positions filled by case examining. Such documents include OF 612, resumes, supplemental forms, whether in hard copy or electronic format.

Cutoff annually. Destroy 2 years after cutoff.

n. Eligible applications for positions filled by case examining that either are not referred to the hiring official or are returned to the examining office by the hiring official. Such documents include OF 612, resumes, supplemental forms, and attachments, whether in hard copy or electronic format.

Cutoff annually. Destroy 2 years after cutoff.

o. Request for prior approval of personnel actions taken by agencies on such matters as promotion, transfer, reinstatement, or change in status, submitted by SF 59, OPM 648, or equivalent form.

Cut off annually. Destroy 1 year after cutoff.

p. Certificate Files, including SF 39, SF 39A, or equivalent, and all papers upon which the certification was based: the list of eligibles screened for the vacancies, ratings assigned, availability statements, the certificate of eligibles that was issued to the selecting official, the annotated certificate of eligibles that was returned from the selecting official, and other documentation material designated by the examiner for retention.

Cut off annually. Destroy 2 years after cutoff.

q. Certification request control index. Certificate control log system. Records of information (e.g. receipt date, series, and grade of position, duty station, etc.) pertaining to requests for lists of eligibles from a register or inventory.

Cut off annually. Destroy 2 years after cutoff.

r. Interagency Placement Program (IPP) application and registration sheet.

Destroy upon expiration of employee's DEP eligibility.

s. DEP control cards, if maintained.

Cut off annually. Destroy 2 years after cut off.

t. Reports of audits of delegated examining operations.

Destroy 3 years after date of the report.

9. Electronic Mail and Word Processing System Copies.

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy.

Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy.

Destroy/delete when dissemination, revision, or updating is completed.