Department of Homeland Security
Office of Inspector General

Management Oversight and Component Participation Are Necessary to Complete DHS' Human Resource Systems Consolidation Effort

OIG-10-99

July 2010

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

JUL - 1 2010

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the actions DHS has taken and progress made to consolidate components' human resource systems into enterprise-wide solutions to achieve greater efficiencies and cost savings. It is based on interviews with selected management officials and contractor personnel, direct observations, system security vulnerability assessments, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	Customs and Border Protection
CIS	Citizenship and Immigration Services
DHS	Department of Homeland Security
EIS	External Information System
E-OPF	Electronic Official Personnel Folder
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
HCBS	Human Capital Business Systems
ICE	Immigration and Customs Enforcement
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OCHCO	Office of the Chief Human Capital Officer

OCIO	Office of Chief Information Officer
OCISO	Office of Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestones
PPS	Pay and Personnel System
TIC	Trusted Internet Connection
TSA	Transportation Security Administration
SaaS	Software as a Service
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USSS	United States Secret Service
WebTA	Web Time and Attendance

Executive Summary

As required by the E-Government Act of 2002 and Office of Management and Budget's (OMB) government-wide initiatives, DHS Office of the Chief Human Capital Officer (OCHCO) began the process, in 2005, to consolidate components' existing human resource information systems into five enterprise-wide solutions. We audited OCHCO to determine the progress DHS has made in consolidating its component human resource information systems in its Human Capital Business Systems (HCBS) unit.

DHS has made some progress in consolidating its human resource systems. Specifically, HCBS has successfully migrated components to the Office of Personnel Management's (OPM) Electronic Official Personnel Folder (e-OPF) system and the United States Department of Agriculture's (USDA) National Finance Center (NFC) Pay and Personnel System (PPS). Further, HCBS has taken steps to coordinate with components to identify business requirements and system specifications for the enterprise-wide systems, including EmpowHR, TalentLink and Web Time and Attendance (WebTA).

However, as of February 2010, components have not migrated from their existing systems to all of the enterprise-wide systems. In addition, HCBS has not implemented adequate performance metrics to track the status of the consolidation effort. Further, enhanced communication and system functionality must be improved to help facilitate the migration of components to the department's enterprise-wide systems. In addition, systems have been certified and accredited without all documents and security weaknesses being mitigated timely. Finally, WebTA has not been certified and accredited according to applicable DHS policy.

We are making 11 recommendations to the Chief Human Capital Officer. OCHCO concurred with all of our recommendations and has already begun to take actions to implement them. The department's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

In 2005, as part of the E-Government Act, OMB implemented a government-wide initiative to eliminate redundancy and increase efficiency in payroll and human resource systems. In response, HCBS led an effort to consolidate components' existing human resource information systems into enterprise-wide solutions aimed at improving security, efficiency, and consistency across the department.

HCBS is responsible for consolidating more than 144 existing component human resource systems into flexible enterprise-wide solutions. While working with components, HCBS is responsible for program management activities, communication and coordination, and integration of information technology tasks for this effort. As part of this initiative, HCBS is in the process of consolidating component human resource systems into five enterprise-wide solutions, including: (1) WebTA, (2) NFC PPS, (3) EmpowHR, (4) TalentLink, and (5) e-OPF system. These systems, which are also used by other federal agencies, support the department with core human resource functions, such as records management, time and attendance, personnel actions, recruitment, and payroll. Figure 1 provides a brief description of each system.

Figure 1-Enterprise-wide Human Resource Solutions

Name	Function	Owner	Description
EmpowHR	Personnel Actions/ Personnel Records	USDA	System interfaces with the NFC's Pay and Personnel System. System functions include creation of new job codes (master records) and positions, reassignments, promotions, and awards.
e-OPF	Personnel Records	OPM	System developed as a management solution to handle official personnel files and simplify employee access to official personnel folders.
NFC PPS	Pay and Personnel	USDA	System used by customer agencies for personnel action processing, position management, benefits processing, payroll, payroll accounting, tax reporting, employee debt management, and reporting.
TalentLink	Recruiting	DHS	System which allows DHS managers and recruiters to facilitate the hiring process.
WebTA	Time and Attendance	DHS	Commercial off-the-shelf system used for time and attendance functions.

Our audit focused on three systems: TalentLink, WebTA, and e-OPF. TalentLink, which is a web-based application, is used by managers, recruiters, and human resource specialists to post job vacancies, select, follow-up and hire potential job applicants. The system is contractor owned and operated and most of the equipment is currently housed at a commercial hosting facility in New York City, New York. According to HCBS personnel, DHS will discontinue the use of TalentLink and switch to a different application in June 2010. WebTA is a web-based, commercial off-the-shelf time and attendance labor solution. The system's functions include electronic approvals, project tracking and activity-base time reporting, on-line leave requests, part-time accrual calculations, year-end leave accruals, rollover and leave transfers. DHS purchased licenses in 2005 and the system is currently hosted by the USDA NFC in Denver, Colorado. The e-OPF system is part of OPM's Enterprise Human Resources Integration initiative. This system provides government employees with direct online access to their official human resource and personnel records.

Due to the sensitive nature of the information stored and processed by these human resource systems, DHS must implement effective controls to protect personal data from potential misuse. According to the United States Government Accountability Office, federal agencies have reported numerous incidents where personally identifiable information was stolen, lost, or improperly disclosed, resulting in loss of privacy and identify theft. To safeguard against stolen or unauthorized disclosure of personal data, OMB requires federal agencies to ensure that proper safeguards are in place to protect personally identifiable information.

Results of Audit

Actions Taken to Implement Enterprise-Wide Human Resource Systems

DHS has taken actions to consolidate and migrate components' human resource systems to the department's enterprise-wide solutions. For example, HCBS has:

- Migrated DHS components to NFC PPS in 2005 and e-OPF in 2008.

- Implemented user and test working groups for DHS components to help identify business requirements and system specifications.

- Certified and accredited TalentLink. Our review of the certification and accreditation package revealed no significant deficiencies.

- Established memoranda of understanding and interconnection security agreements with NFC and OPM to define roles and responsibilities for the management, operation, and security of system connections.

- Implemented effective controls to protect the sensitive data stored and processed by TalentLink. Our security testing revealed only a few areas in need of improvement.

Despite these actions, DHS faces additional challenges with implementing all of the enterprise-wide human resource solutions at its components. For example, many DHS components are reluctant to adopt the department's enterprise-wide solutions. More work remains to ensure that components' existing human resource systems are consolidated into the department's enterprise-wide solutions.

Management Oversight Is Needed to Complete the Consolidation of DHS' Human Resource Systems

DHS has made some progress, but has not completed its human resource system consolidation effort. Senior DHS officials need to provide better guidance and oversight to migrate components to the department's enterprise-wide human resource solutions. Component officials stated that system functionality issues and insufficient communication with HCBS contributed to their reluctance to migrate. Further, DHS has not restricted its external internet connections or maintained an accurate inventory of its human resource systems, preventing the department from achieving its efficiency objectives. Unless these issues are addressed, DHS may not be able to achieve its goal of consolidating and modernizing its human resource systems.

Components Are Reluctant to Implement Enterprise-Wide Systems

As of February 2010, nine DHS components have not completed their migration to WebTA, EmpowHR, or TalentLink.[1] Component officials indicated that some of the enterprise-wide solutions do not satisfy their business requirements and the lack of detailed cost savings information from HCBS has prevented them from migrating. Consequently, components continue to use their existing systems in lieu of the DHS enterprise-wide solutions. Figure 2 summarizes the implementation status for the three systems.

Figure 2-System Consolidation Progress

	TalentLink	EmpowHR	WebTA
Components			
CBP	Not Started	Not Started	Not Started
CIS	Not Started	Not Started	In progress
FEMA	In progress	Not Started	Complete
FLETC	In progress	Complete	Complete
ICE	In progress	Not Started	Complete
NPPD	In progress	Complete	Complete
TSA	Not Started	Complete	Complete
USCG	Not Started	Complete	Complete
USSS	Not Started	Not Started	Complete

Additional Oversight Is Needed

Prior to January 2010, senior DHS officials had not issued any guidance to components on its human resource consolidation effort. Without the guidance, HCBS could not compel all components to migrate towards the enterprise-wide solutions. As a result, the progress to date

[1] The nine components are Customs and Border Protection (CBP), Citizenship and Immigration Services (CIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration and Customs Enforcement (ICE), National Protection and Programs Directorate (NPPD), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS)

has been limited as some components are reluctant to migrate to DHS' enterprise-wide human resource systems.

On January 15, 2010, the Deputy Secretary issued a memorandum tasking OCHCO and Office of Chief Information Officer (OCIO) to assemble and integrate a project team to rationalize legacy human resource processes and systems into a department-wide architecture.[2] As outlined in the memorandum, components are prohibited from spending additional funding to purchase new or enhance existing human resource systems without the approval from either OCHCO or OCIO. The issuance of this memo will help HCBS to complete its human resource consolidation effort by providing additional oversight authority over components. For example, as mandated under the E-Government Act of 2002 and OPM's initiatives, HCBS has successfully facilitated the migration of NFC PPS and e-OPF throughout DHS.

The lack of oversight authority over the components has also hindered HCBS' ability to implement the human resource consolidation initiative. For example, HCBS does not have the authority to review components' budgets to ensure that adequate resources are available for the initiative. According to HCBS personnel, some components have not fully engaged in the planning and implementation activities required to complete the initiative. For example, during the formative stages, components are willing to participate and engage in system planning and requirements analysis activities. However, once HCBS begins the implementation and acquisition activities, components often withdraw from the initiative stating that: (1) they are not ready to begin the migration effort, (2) they do not have sufficient resources to support the migration, or (3) the enterprise-wide solutions do not meet their mission or business requirements. In addition, HCBS personnel have stated that leadership changes at OCHCO and components that lead to different management priorities have slowed the migration efforts.

[2] *DHS Enterprise Human Resources Processes, People, and Technology* Memorandum, dated January 15, 2010.

As part of DHS' policy for exchanging and sharing internal information, components are required to standardize the information technology assets used to access, store, process, and manage its information. To achieve this goal, including standardization of its human resources assets, DHS must provide OCHCO with adequate oversight authority; otherwise it will be restricted from consolidating information systems and infrastructure used to support the department's human resource operations.

Performance Metrics

HCBS has not developed adequate performance metrics to track the overall progress of the consolidation effort. Performance metrics are used to evaluate the progress of a program or project and ensure that key milestones and goals are being achieved.

While HCBS has developed performance measures to evaluate the technical performance of the department's enterprise-wide systems, it does not have metrics to track the overall progress of the initiative. For example, HCBS keeps current metrics on security incidents, service desk tickets, and system release data. In addition, HCBS tracks the number of users and components that have migrated to the enterprise-wide solutions on a quarterly basis. However, HCBS has not developed performance metrics to track the status of component requirements, interim tasks, or activities that must be completed to ensure that components successfully migrate to the enterprise-wide systems.

Specific performance metrics can help HCBS track the overall progress of the implementation effort rather than the technical performance of individual systems. Examples of additional performance metrics may include:

- Key requirements, milestones and accomplishments that have or have not been completed.

- Required deliverables or services that have or have not been completed.

- Remaining tasks that must be completed.

Performance metrics aimed at assessing the completion of component implementation requirements or activities will help HCBS personnel monitor the overall progress of the consolidation effort. In addition, such metrics will allow HCBS to determine the areas where additional focus is required.

OMB requires agencies to implement performance metrics for planning, budgeting, and managing federal capital assets. These performance metrics should be used to monitor and compare expected results with actual performance of the project.

Without specific performance metrics, it will be difficult for program officials to determine the overall progress of the project and whether expected results or outcomes have been achieved. In addition, detailed performance metrics will provide DHS with the ability to better monitor the components' implementation progress and identify areas where improvements should be made.

System Functionality and Communication Can Be Improved

Components have cited functionality issues with the enterprise-wide systems and insufficient communication with HCBS as reasons for not migrating to all of the enterprise-wide solutions. For example, some components have identified functionality deficiencies with the enterprise-wide human resource systems, including issues with vacancy announcements and the certification process.[3] In addition, component officials stated that communication with HCBS regarding the consolidation effort could be improved. Specifically, HCBS should identify detailed cost savings to illustrate to components' the potential benefits of migrating to the department's enterprise-wide solutions.

[3] The certification process is used by hiring managers to identify a list of the best qualified applicants that may be considered for a vacancy announcement.

We met with selected personnel from component human resource offices and OCIO to identify possible concerns regarding the consolidation effort. Some components have indicated that the department's enterprise-wide solutions do not satisfy their business requirements and that they have encountered functionality issues with some of the systems. Specifically, FEMA and NPPD have encountered issues with TalentLink and requested to replace the system with another system. FEMA indicated that TalentLink does not consistently post vacancy announcements to USAJobs and contains too many steps in the certification process.[4] This cumbersome process has lengthened the amount of time for human resource staff to develop certificates containing the best qualified candidate lists. Similarly, NPPD stated that hiring managers experienced difficulty in reviewing the certificates of eligible applicants and often found that other critical documents such as resumes were inadvertently being removed from job applications. In addition, NPPD indicated that it takes nearly three times as long to post a vacancy position using TalentLink as in NPPD's current system, USA Staffing. According to HCBS personnel, OCHCO is planning to discontinue the use of TalentLink in June 2010, as the department is participating in an OPM initiative to develop a new recruiting system that better suits federal agencies' needs.

Components also expressed concerns with EmpowHR and stated that they will not implement the system until it is equal to or better in terms of functionality and cost than their current systems. For example, USSS does not plan to adopt EmpowHR until HCBS provides sufficient information to convey the benefits of retiring HRConnect.[5] TSA has also encountered functionality issues when using EmpowHR. For example, when information is edited with a front-end system other than EmpowHR, the data changes will be updated in NFC's mainframe computer but not in EmpowHR's database tables. Consequently, the data stored in the NFC mainframe and EmpowHR's database tables become inconsistent. As a result, dual entries must

[4] USAJobs is an OPM system used to post job openings for the federal government. It interfaces with TalentLink.

[5] HRConnect provides USSS with quick hire staffing solutions and handles personnel transactions.

be performed to correct the discrepancies which results in additional costs and time to TSA.

HCBS personnel said that they have been working with NFC to remediate the deficiencies identified by the components. According to HCBS personnel, they have stopped deploying EmpowHR at components until the deficiencies identified are resolved.

Finally, four components (CBP, NPPD, TSA and USSS) said that HCBS has not communicated effectively or accurately about the potential cost savings of migrating to the enterprise-wide solutions. As a result, components are reluctant to replace their current systems with the department's enterprise-wide solutions until HCBS identifies projected cost savings.

As part of the E-Government Act, agencies are required to make use of information technologies, including the reduction of duplicate and fragmented systems. To meet this requirement and complete the human resource consolidation effort, HCBS must continue to work with components to address the deficiencies in system functionality. In addition, HCBS must convey the detailed cost savings to components and provide them with systems that adequately meet their needs. Unless these tasks are achieved, DHS cannot complete the consolidation effort.

Human Resource System Inventory

HCBS has not identified all human resource systems at the components. Without an accurate inventory of human resource systems, HCBS cannot determine whether components are using redundant systems.

While HCBS maintains a list of the department's human resource systems, it is outdated and inaccurate. According to HCBS personnel, the inventory list has not been updated since 2007. In addition, HCBS officials stated that components are not obligated to respond to HCBS' information requests to update its inventory list of human resource systems. As a result, components provided either limited information or did not respond at all. As of

December 2009, HCBS' inventory list identifies 58 unique human resource systems.

In October 2009, we requested components to identify their human resource systems and to evaluate the accuracy of systems maintained by HCBS. In response, components identified a total of 48 human resource systems. We attempted to verify the information obtained with the system inventory maintained by DHS OCIO. However, the DHS OCIO inventory does not have an identifier to distinguish those systems that process human resource functions, such as records management, time and attendance, personnel actions, recruitment, and payroll functions. Without the identifier, we could not evaluate the accuracy of information obtained. The discrepancy between HCBS' inventory and the responses to our data call is an indicator that DHS cannot account for all of its human resource systems.

Components Maintain Network Connections Outside of DHS Trusted Internet Connections

As of March 2010, 5 components maintained 11 external network connections to NFC that are outside of the DHS trusted internet connections (TIC). These connections provide users with access to personnel systems owned and housed at NFC, including WebTA, EmpowHR, and NFC PPS. Figure 3 provides an overview of the external connections that are maintained by components.

Figure 3-External Connections to NFC

Component	Number of External Network Connections
FEMA	3
TSA	6
CBP/FLETC	1 (shared)
USCG	1
Total	**11**

We attempted to verify the number of connections with NFC and components. However, we were unable to reconcile the differences between the information provided by NFC and the components. According to an HCBS official, DHS does not have adequate visibility over its components' external network connections. However, HCBS is working with OCIO to consolidate existing component connections.

In November 2007, OMB required agencies to consolidate internet points of presence and reduce external network connections to improve efficiency and security.[6] DHS OCIO aligns OMB's TIC initiative with its OneNet consolidation project.[7] By allowing components to maintain their own network connections to NFC, it contradicts OMB's TIC and DHS OneNet initiatives to improve efficiency and security by reducing the internet points of presence. These connections increase the number of internet points of presence and may pose a security risk to department data if security controls are inadequate.

Recommendations:

We recommend that the OCHCO direct HCBS to:

Recommendation #1: Develop specific performance metrics to help track the overall progress of the consolidation effort.

Recommendation #2: Improve communication and coordination with components to address system functionality issues and convey detailed cost savings for system migration.

Recommendation #3: Work with DHS OCIO and components to identify and track all human resource systems.

Recommendation #4: Coordinate with OCIO to ensure that components comply with OMB TIC and DHS OneNet initiatives to reduce internet points of presence for human resource connectivity.

Management Comments and OIG Analysis

DHS concurred with recommendation 1. OCHCO indicated that, with the change in leadership and direction, it is currently revising the OMB Exhibit 300, operational plan, and program metrics.

[6] OMB memorandum 08-05, *Implementation of Trusted Internet Connections*, dated November 20, 2007.

[7] The purpose of OneNet is to consolidate and standardize a network architecture and improve cost effectiveness across the enterprise. OneNet will eventually integrate with component wide area networks to reduce the number of fragmented component networks and provide DHS with a secure, in-house global communications solution with centralized management and configuration capabilities.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 2. In its response, OCHCO indicated that project teams are working with component functional experts to define and develop requirements. Furthermore, HCBS is currently reworking the intake and change control process to better accommodate changes and requests in real-time. Improved metrics capability will also enhance OCHCO's ability to consistently deliver cost data during different stages of the project. Finally, a strategic Human Resources Information Technology Council is also being established to improve communication and component feedback.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 3. OCHCO responded that it will work with OCIO to create a unique identifier within the department's system inventory tool to identify human resources systems.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 4. In its response, OCHCO indicated that OCHCO and OCIO are working with components to determine the business requirements and bandwidth usage, and to identify and implement the appropriate type and set of DHS OneNet connections that are required to process NFC payroll and personnel transactions.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Enhancements Can Be Made to TalentLink's Technical Controls

Overall, the controls implemented on TalentLink were effective to protect the sensitive data stored and processed by the system. Our evaluation included testing for vulnerabilities on the database and selected servers and network devices for compliance with DHS guidance. In addition, we manually reviewed system configurations and interviewed system administrators on system management processes. Our security testing and analysis revealed that improvements can be made to administrator account management, system management procedures, and configuration settings. DHS needs to address these issues to reduce the security risks to its human resource systems.

Administrator Accounts are Inadequately Managed

DHS has not implemented effective controls on administrator accounts to ensure that they are granted with the least privileges to perform their job functions. In the event of a security incident, the scope of potential damage to the system increases as users are granted excessive access privileges. A security incident targeting an administrator account might include an authorized user abusing his or her access or exploitation from an outsider gaining unauthorized control of an account. For example:

- Administrators' connections to servers are not timed out after more than 30 minutes of inactivity. In most cases, these accounts are not locked out until after 60 minutes or 24 hours of inactivity. According to system administrators, this extended log-in time is needed to keep administrative tasks active for extended periods of time, such as file transfers to the logging server. An HCBS official indicated that the system is intentionally misconfigured for the convenience of administrative tasks. OMB requires that remote users accessing personally identifiable information be re-authenticated after 30 minutes of inactivity. DHS requires that user sessions be terminated after 60 minutes of inactivity to protect sensitive data.

- The Oracle remote login password file is in use, which allows remote administrators to automatically authenticate to the database without entering username and password. According to an HCBS official, this is an oversight that the remote login password file is still in use. DHS requires that the Oracle remote login password file be disabled to enforce server-based authentication of users connecting to the database.

- Six accounts have been granted the elevated CREATE ANY LIBRARY privilege in the Oracle database, while there are only two database administrators for TalentLink. The CREATE ANY LIBRARY privilege allows an Oracle user to define a library, or code and data. An attacker could use it to access the operating system. HCBS officials could not provide an explanation why the other four accounts were granted the elevated privilege. Database administrators are granted privileges to create new databases and alter and delete data. DHS requires that access permissions including CREATE ANY LIBRARY be restricted to database administrators. Further, DHS requires that users' access be restricted to the least privilege to perform job duties.

Elevated access to system resources and data should be limited and managed appropriately. Without effective measures to restrict access to servers and sensitive data, DHS may be at risk of an individual engaging in fraudulent or malicious behavior resulting in unauthorized alteration, loss, unavailability, or disclosure of information.

Patch and Privileged Account Management Processes

The procedures for patch management and privileged account management processes have not been developed for TalentLink. DHS requires that a policy be developed to define the roles and responsibilities of the patch management process and deployment status. DHS also requires that user access be documented in access control policies and procedures. Both tasks are controlled by HCBS personnel who considered formal, step-by-step directions unnecessary.

Documenting processes will help personnel identify, understand, and consistently implement requirements, minimizing the risk of human error. In the event of staffing or contract changes, patching and privileged account management processes may be neglected due to lack of documented procedures. Unmanaged privileged accounts and missing patches leave the system at risk of user abuse and external cyber attack.

Process for Destruction of Personally Identifiable Information Extracts

HCBS has not implemented a process for destroying computer-readable personally identifiable information extractions. Specifically, TalentLink allows users to extract personal information in the form of reports on various hiring statistics and information. OMB requires that agencies ensure computer-readable data extracts that contain personally identifiable information be erased within 90 days or when no longer needed. However, HCBS staff considers that it would be infeasible to ensure that all personal information extractions are erased as users are spread throughout DHS and cannot operate without reports.

Enforcing the destruction of personally identifiable information extractions helps reduce the amount of sensitive data that is physically removed from department locations or that is accessed remotely. Destroying extracts also prevents misuse of sensitive data.

Database and Server Configuration

The TalentLink Oracle database and servers are not configured according to DHS policy. We identified deficiencies in configuration settings that may lead to unauthorized misuse of sensitive data. Specifically:

- Audit trails are not enabled on the Oracle database to track user account activity. DHS requires that audit trails be enabled to capture detailed user activity records in the database. User access, use of system privileges, and changes to the database should be logged to help investigate and reconstruct future security incidents.

- A contractor's warning banner is used instead of the required DHS banner during server logins. DHS requires that a specific login warning banner be displayed when connecting to a system to remind users of their responsibilities in using government-owned equipment.

- A high-risk vulnerability that has been identified since 2004 was found on an application server. The JBoss software running on the application server is configured in a way that allows unauthenticated access to certain administrative functions of the software.[8] A remote attacker could exploit the vulnerability to disclose sensitive information or take control of JBoss. DHS requires that software patches be applied in a timely manner to protect the system from known exploits.

Audit trails are essential to the investigation and reconstruction of security incidents. In particular, access to personal data in the Oracle database should be closely tracked, with all actions tied to individual users. The lack of audit trails combined with excessive privileges granted to database users puts the system at significant risk of data misuse. Violations could go unnoticed or may not be traceable to individual users once discovered.

Memorandum of Agreements With Other Agencies

While HCBS has established memorandum of agreements with NFC and OPM, the agreements do not contain terms that will allow DHS and OIG unrestricted access to system specific resources, such as vulnerability scan results, appropriate technical staff, and information related to system connections between NFC and DHS. Unrestricted access to the information is essential to verify that effective controls have been implemented on DHS' human resource systems that are owned and operated by other agencies.

As part of our original audit scope, we planned to perform security testing to evaluate the effectiveness of controls implemented on all enterprise-wide systems. However, USDA and OPM personnel were reluctant to provide us with access to the information for the systems selected for review, i.e., NFC testing results, connections between NFC and components. The limitations restricted our ability to perform planned security testing. For example, NFC indicated that the agency does not plan to allow other federal agencies to perform security testing on systems that it maintains.

Without such access, HCBS cannot ensure that security tests are being performed periodically and that effective controls have been implemented on its human resource systems. Unless HCBS revises its existing memoranda of agreement to include the provisions for unrestricted access to system specific information,

[8] JBoss is a software framework for an application server that supports Java application development.

DHS cannot guarantee that all applicable security requirements have been met for its human resource systems which are owned and operated by other agencies.

Recommendations:

We recommend that the OCHCO direct HCBS to:

Recommendation #5: Develop policies for patch management, privileged account management, and the destruction of personal data extracts for TalentLink.

Recommendation #6: Restrict TalentLink administrator access permissions by granting the least privileges needed to perform job functions in accordance with applicable OMB and DHS policy.

Recommendation #7: Configure TalentLink's database and servers according to DHS policy.

Recommendation #8: Revise existing memoranda of understanding with other agencies to ensure that system specific information is available to HCBS and the OIG.

Management Comments and OIG Analysis

DHS concurred with recommendation 5. OCHCO commented that, due to the Software as a Service (SaaS) provision of TalentLink, the patch management and privileged account management processes are owned by the application provider. HCBS reviewed these processes and validated they were consistent with DHS requirements. However, to be consistent with DHS policy, OCHCO concurred that HCBS should have drafted TalentLink-specific patch management and privileged account management SOPs and utilized the application provider documents as the basis. Since OCHCO will discontinue the use of TalentLink in June 2010, HCBS does not plan to create a Plan of Action and Milestones (POA&M) to develop policies for a system that will soon be retired.

Regarding personal data extracts, OCHCO responded that while the protection of computer-readable extracts containing personally identifiable information was incorporated in DHS guidance before TalentLink went live, the implementation directive was not published until July 31, 2009. Thus, HCBS was not able to complete a thorough analysis to determine what computer-readable extracts (routine or ad hoc) would be utilized by the system prior to the decision to decommission the system. All users of the system are required to complete annual Computer Security Awareness Training and Privacy Training, so users are trained in the proper handling of personally identifiable information.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 6. Regarding the Administrator's Connections and Oracle Remote Login Password File, OCHCO responded that due to the SaaS provision of this system, certain configurations are beyond the control of DHS. OCHCO was aware of this issue, but the application provider was not willing to change the settings as it would cause undue burden on the application's operating capability. Due to the fact that the TALENTLink system is being decommissioned and will be shut-down on June 26, 2010, HCBS does not plan to create a POA&M to correct the deficiency.

Regarding the elevated Oracle Accounts, OCHCO responded that there are a total of eight accounts, comprised of two database administrators and six users, with the "CREATE ANY LIBRARY" privilege. The six user accounts must exist on each of the application provider databases so that the application can be operated correctly and, since the six users do not require full database administrator access, limiting these accounts to this privilege is actually more restrictive and in-line with the concept of Least Privilege. The alternative would be to grant these six users full DBA access, but this would give them more privileges than required.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 7. Regarding the audit trails and warning banner findings, OCHCO responded that due to the

SaaS provision of TalentLink, certain configurations are beyond the control of DHS. Although the Oracle Hardening guide is not strictly adhered to, there are other tracking capabilities built into the application to allow auditing. Additionally, although the proper warning banner is not provided when logging on locally to the server, the proper DHS warning and privacy banners are provided for all users and candidates accessing the system. According to OCHCO, HCBS was aware of these issues, but the application provider was not willing to change the settings because it would cause undue burden on the application's operating capability. Since OCHCO will discontinue the use of TalentLink in June 2010, HCBS does not plan to create a POA&M to correct the deficiencies for a system that will soon be retired.

Regarding the JBoss vulnerability, OCHCO commented that the weakness was identified prior to the OIG scan. Subsequently, a new system build was subsequently required for TalentLink. However, the new system build was not consistently deployed prior to the OIG scan. The vulnerability has since been remediated in all zones.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 8. OCHCO responded that while OCHCO agrees with the intent of the recommendation, DHS policy does not support the performance or security testing on another agency's IT systems. Based on DHS policy, the connection is to be well-documented with emphasis on the responsibilities of the two organizations including maintaining a valid authority to operate, incident reporting, training and awareness, etc. OCHCO will include specific language in future Memoranda of Agreement/Understanding to document mutual responsibility and roles for security systems.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Certification and Accreditation Deficiencies Identified in Human Resource Systems

HCBS has not ensured that all OMB and DHS security requirements are met on its enterprise-wide human resource systems. Specifically, e-OPF has been certified and accredited without all required security documents. In addition, while POA&Ms are being created to track and identify security weaknesses, the corrective actions for one third of the POA&Ms are more than 90 days past due. Further, WebTA has not been certified and accredited in accordance with applicable DHS policy.

Certification and Accreditation Documentation is Incomplete

Our review of the e-OPF certification and accreditation packages revealed that not all of the required security documents have been developed. For certification and accreditation purposes, OPM divided e-OPF into: (1) a front end application, (2) the Chantilly Scanning Facility, and (3) the Ashburn Data Center systems. We reviewed the accreditation packages for the e-OPF front-end application and Chantilly Scanning Facility for compliance with applicable OMB and National Institute of Standards and Technology (NIST) guidance. Configuration management plans were not developed for either system. Configuration management plans provide guidance to ensure that any subsequent change to a system is approved and that all recommended and approved security patches are properly installed.

Agencies are required to certify and accredit their systems in accordance with OMB and NIST guidance, including all security artifacts. Certification and accreditation requirements must also be satisfied for systems owned and operated by outside agencies or contractors.

According to HCBS officials, they have tried to maintain appropriate adherence to certification and accreditation standards for systems that are owned and operated by contractors including e-OPF, WebTA, and TalentLink. However, they have had difficulty in performing continuous monitoring functions, detailed reviews, and yearly site visits on contractor systems due to limited staffing. Further, HCBS relies solely on its yearly site visits to ensure that human resource systems comply with certification and accreditation package protocol and guidance.

Without configuration management plans, program officials cannot ensure that e-OPF has been properly configured and that security patches are applied periodically. Therefore, DHS has limited assurance that the sensitive information of its employees is secured in accordance with applicable policies.

Security Weaknesses Are Not Being Mitigated In a Timely Manner

Security weaknesses in e-OPF POA&Ms are not being maintained or mitigated in a timely manner. As of February 22, 2010, the corrective actions for 28 of 110 POA&Ms are more than 90 days overdue. In addition, 21 of these overdue POA&Ms are more than one year past due and four are classified as “critical”. Critical security weaknesses should be mitigated in a timely manner to ensure that they cannot be exploited to gain unauthorized access to the system.

Agencies are required to create POA&Ms for all known security weaknesses that cannot be immediately mitigated. In addition, POA&Ms are part of the continuous monitoring process to ensure that security weaknesses are mitigated timely. Further, OMB requires POA&Ms be prioritized in varying levels of criticality depending on how management categorizes the weakness in order to efficiently and effectively protect systems.

Without the timely mitigation of POA&Ms, agencies cannot ensure that security weaknesses are properly addressed before they can be exploited. Security weaknesses not mitigated timely may expose the personal data of DHS employees.

WebTA Has Not Been Certified and Accredited in Accordance with DHS Policy

As of March 2010, WebTA had not received the authority to operate in accordance with DHS policy. For Federal Information Security Management Act reporting purposes, the Office of Chief Information Security Officer (OCISO) reviews accreditation packages for all systems in the systems inventory for compliance with applicable DHS and NIST guidance. Without the OCISO's validation of certification and accreditation artifacts, a system operates without authority.

WebTA was originally certified and accredited by NFC in October 2006. In August 2009, HCBS and NFC agreed that DHS should certify and accredit the system as the department owns the WebTA licenses and data. Specifically, HCBS purchased the license for WebTA in 2005 for $1,000,000 and pays the annual maintenance cost of $802,000.[9] Subsequently, the WebTA authorizing official certified and accredited the system in October 2009.[10] However, security personnel from the Management Directorate disagreed with the assessment and removed WebTA from DHS OCIO's systems inventory in October 2009. Security personnel from the Management Directorate indicated that DHS does not have control over WebTA because it is hosted on NFC's infrastructure, preventing them from performing detailed tests or configurations. As a result of WebTA's exclusion from DHS' system inventory, OCISO has not recognized the system's authority to operate. However, this exclusion is not justified. WebTA should be included in OCIO's system inventory because the department owns the WebTA license and is responsible for protecting the personal data of its 180,000 employees.

According to DHS inventory guidance, a system's owner is based primarily on system ownership and funding, which HCBS is responsible for since the deployment of the system. According to applicable OMB and DHS guidance, information systems are to be accounted for in agencies' inventory and must be authorized to operate.

[9] Annual maintenance estimate was determined by averaging DHS' WebTA maintenance cost over a five-year period.

[10] An authorizing official assumes responsibility for operating an information system at an acceptable level of risk.

Recommendations:

We recommend that the OCHCO direct HCBS to:

Recommendation #9: Establish a process to ensure that all contractor owned and operated human resource systems are certified and accredited according to applicable OMB and NIST guidance. In addition, all required security documents must be developed according to applicable OMB and NIST guidance, and security weaknesses identified must be mitigated timely.

Recommendation #10: Strengthen the department's monitoring oversight of POA&Ms for non-DHS human resource systems.

Recommendation #11: Certify and accredit WebTA to operate according to applicable OMB, NIST, and DHS guidance.

Management Comments and OIG Analysis

DHS concurred with recommendation 9. According to OCHCO, the human resources systems cited in the report are considered External Information Systems (EIS). These systems are managed by another government agency and are provided as a paid service for DHS use. The responsibility for performing certification and accreditation on these systems is solely that of the host government agency. OCHCO will strengthen the Memorandum of Agreements/Understanding between the other government agencies to clearly delineate the responsibility for the systems to be squarely on the host government agency and that results are available to OCHCO.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 10. OCHCO responded that the human resources systems cited in the report are considered EIS. These systems are managed by another government agency and are provided as a paid service for DHS use. The responsibility for security and management of these systems is solely that of the host government agency. The POA&M deficiencies noted in this report are not DHS specific, and OPM has made significant progress in closing more than 100 POA&Ms noted during prior year assessments of the systems.

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS concurred with recommendation 11. OCHCO responded that WebTA is currently being recorded in the OCIO inventory as an EIS. The system is managed by USDA as part of their mandate to be a provider of this type of service for other government agencies. The responsibility for security and management of this system is clearly delineated as USDA's responsibility. However, OCHCO noted that HCBS must decide whether to accept the NFC line of software codes. The decision will determine whether NFC or DHS should assume the ownership as well as the responsibility to certify and accredit the system. Currently, HCBS is working with OCIO to have the issue resolved.

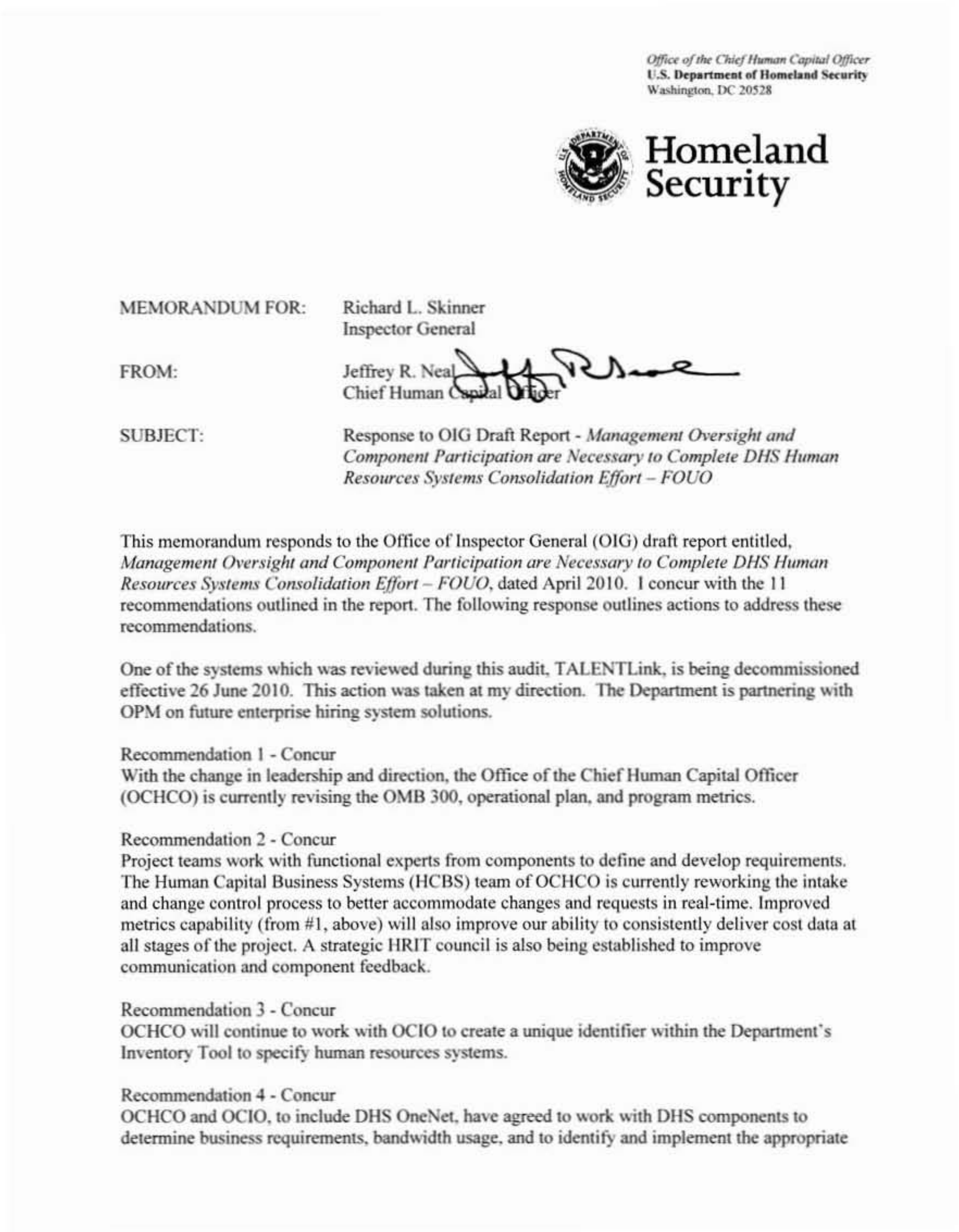
We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open until DHS provides documentation to support that all planned corrective actions are completed.

The objective of our review was to determine whether DHS has developed a program to improve the efficiency, effectiveness, and consistency of its human resource systems. Specifically, we determined whether: (1) DHS has developed an adequate strategy to consolidate components' existing human resource systems into an enterprise-wide solution; (2) DHS has implemented effective physical and system security controls to protect sensitive information stored and processed by its human resource systems; and (3) the enterprise-wide system, including those owned and operated by other agencies, were certified and accredited in accordance with applicable guidance.

We interviewed selected personnel from DHS OCHCO, USDA NFC, major components, Department of the Treasury Bureau of Public Debt in Parkersburg, West Virginia and at one contractor facility in New York City, New York. Further, we reviewed and evaluated DHS' security policies and procedures, system project plans, technical descriptions, certification and accreditation packages, and other appropriate documentation. In addition, we reviewed USDA's *Statement on Auditing Standards No. 70 Report on National Finance Center General Controls - Fiscal Year 2009* to ensure NFC systems were certified and accredited and no major deficiencies were identified. We used software tools, Nessus and DBProtect, to detect, analyze, and evaluate the effectiveness of the security controls implemented on selected human resource systems to identify known security vulnerabilities and evaluate whether systems are properly configured in accordance with applicable guidance. Due to limitations for systems owned and operated by other agencies, we only performed security testing on TalentLink.

We conducted this audit between October 2009 and April 2010 according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Major OIG contributors to the audit are identified in Appendix C. The principal OIG points of contact for the audit are Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4100, and Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Appendix B
Management Comments to the Draft Report



Office of the Chief Human Capital Officer
U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Jeffrey R. Neal
Chief Human Capital Officer

SUBJECT: Response to OIG Draft Report - *Management Oversight and Component Participation are Necessary to Complete DHS Human Resources Systems Consolidation Effort – FOUO*

This memorandum responds to the Office of Inspector General (OIG) draft report entitled, *Management Oversight and Component Participation are Necessary to Complete DHS Human Resources Systems Consolidation Effort – FOUO*, dated April 2010. I concur with the 11 recommendations outlined in the report. The following response outlines actions to address these recommendations.

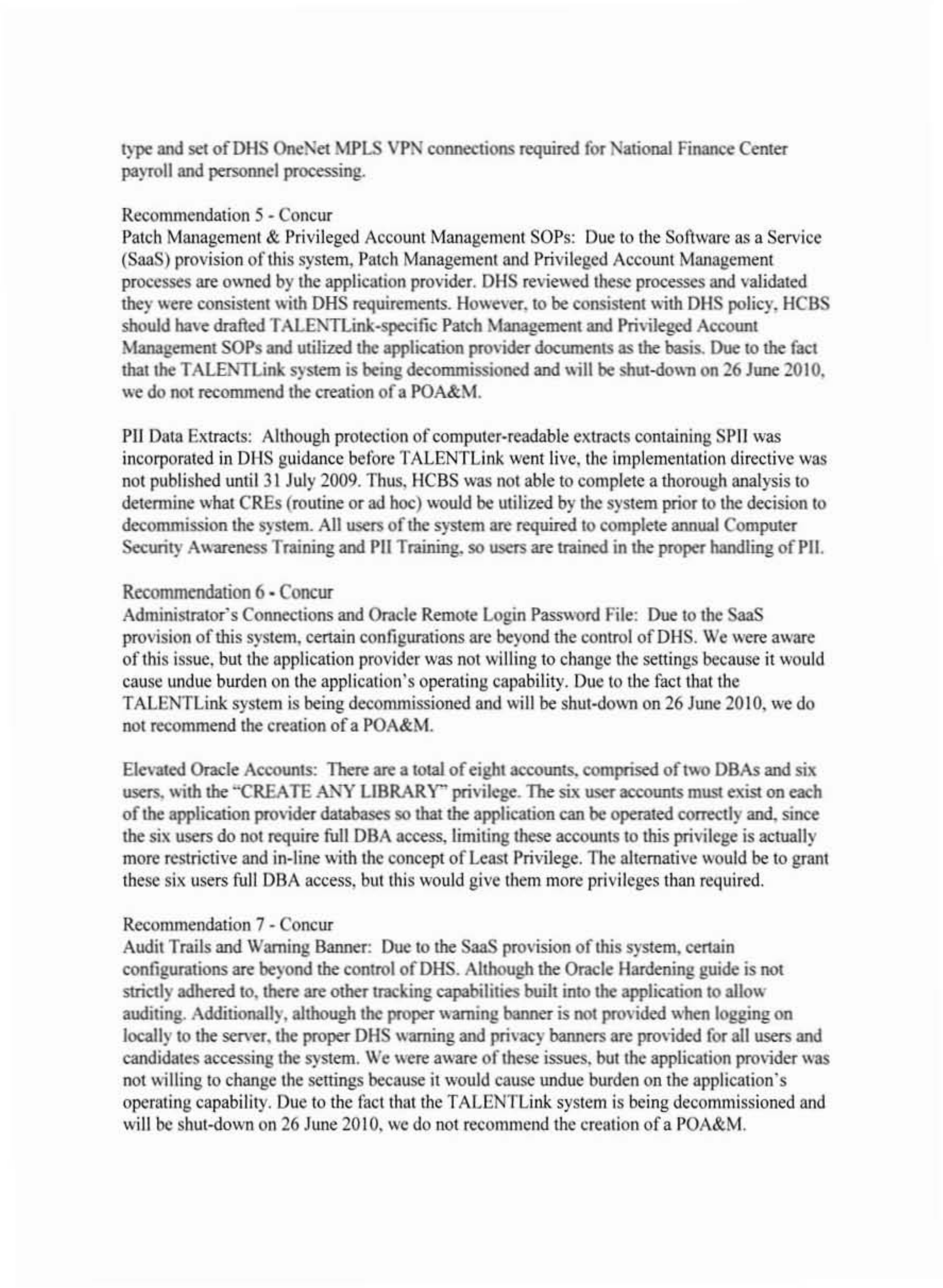
One of the systems which was reviewed during this audit, TALENTLink, is being decommissioned effective 26 June 2010. This action was taken at my direction. The Department is partnering with OPM on future enterprise hiring system solutions.

Recommendation 1 - Concur
With the change in leadership and direction, the Office of the Chief Human Capital Officer (OCHCO) is currently revising the OMB 300, operational plan, and program metrics.

Recommendation 2 - Concur
Project teams work with functional experts from components to define and develop requirements. The Human Capital Business Systems (HCBS) team of OCHCO is currently reworking the intake and change control process to better accommodate changes and requests in real-time. Improved metrics capability (from #1, above) will also improve our ability to consistently deliver cost data at all stages of the project. A strategic HRIT council is also being established to improve communication and component feedback.

Recommendation 3 - Concur
OCHCO will continue to work with OCIO to create a unique identifier within the Department's Inventory Tool to specify human resources systems.

Recommendation 4 - Concur
OCHCO and OCIO, to include DHS OneNet, have agreed to work with DHS components to determine business requirements, bandwidth usage, and to identify and implement the appropriate



type and set of DHS OneNet MPLS VPN connections required for National Finance Center payroll and personnel processing.

Recommendation 5 - Concur
Patch Management & Privileged Account Management SOPs: Due to the Software as a Service (SaaS) provision of this system, Patch Management and Privileged Account Management processes are owned by the application provider. DHS reviewed these processes and validated they were consistent with DHS requirements. However, to be consistent with DHS policy, HCBS should have drafted TALENTLink-specific Patch Management and Privileged Account Management SOPs and utilized the application provider documents as the basis. Due to the fact that the TALENTLink system is being decommissioned and will be shut-down on 26 June 2010, we do not recommend the creation of a POA&M.

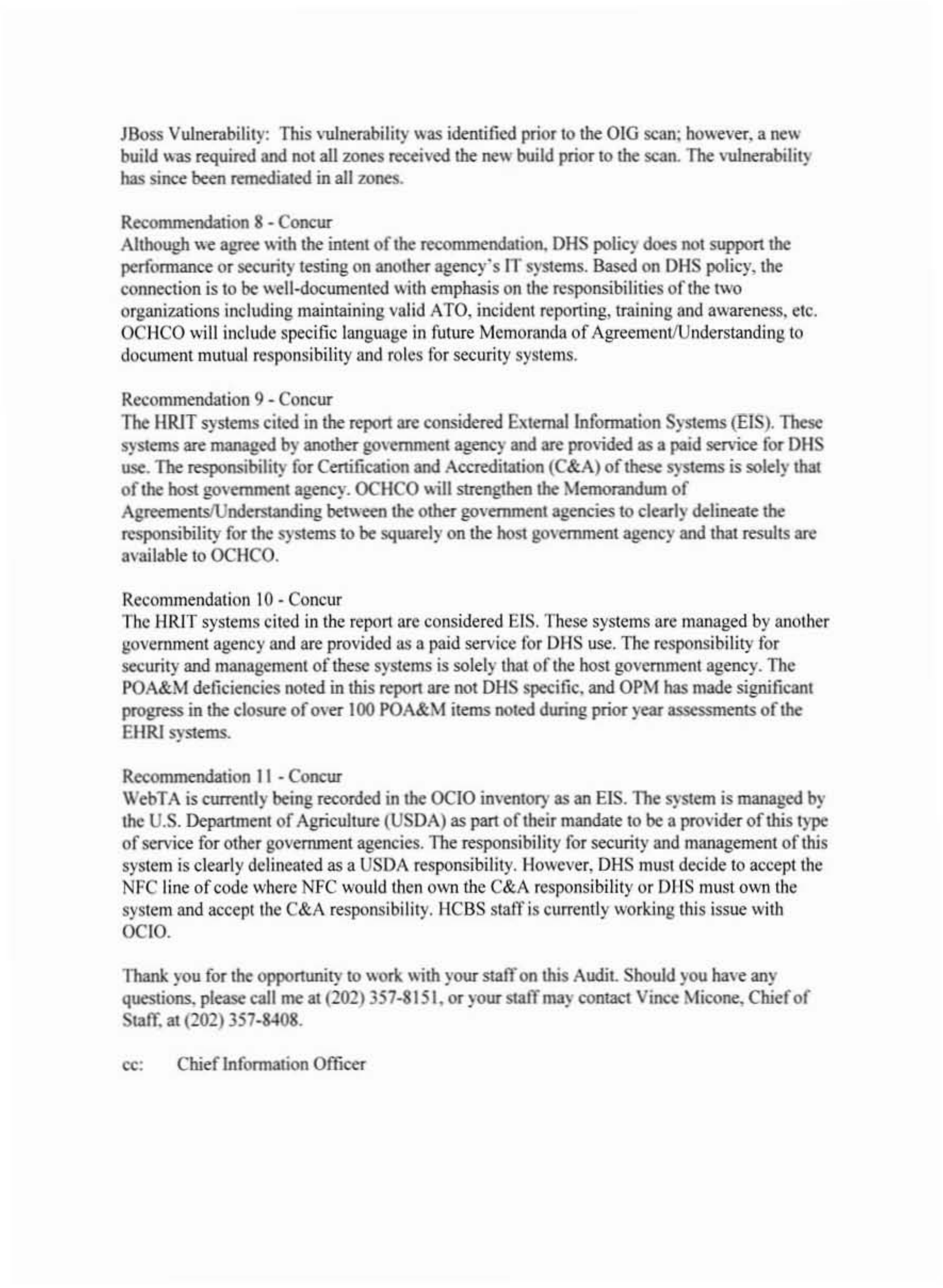
PII Data Extracts: Although protection of computer-readable extracts containing SPII was incorporated in DHS guidance before TALENTLink went live, the implementation directive was not published until 31 July 2009. Thus, HCBS was not able to complete a thorough analysis to determine what CREs (routine or ad hoc) would be utilized by the system prior to the decision to decommission the system. All users of the system are required to complete annual Computer Security Awareness Training and PII Training, so users are trained in the proper handling of PII.

Recommendation 6 - Concur
Administrator's Connections and Oracle Remote Login Password File: Due to the SaaS provision of this system, certain configurations are beyond the control of DHS. We were aware of this issue, but the application provider was not willing to change the settings because it would cause undue burden on the application's operating capability. Due to the fact that the TALENTLink system is being decommissioned and will be shut-down on 26 June 2010, we do not recommend the creation of a POA&M.

Elevated Oracle Accounts: There are a total of eight accounts, comprised of two DBAs and six users, with the "CREATE ANY LIBRARY" privilege. The six user accounts must exist on each of the application provider databases so that the application can be operated correctly and, since the six users do not require full DBA access, limiting these accounts to this privilege is actually more restrictive and in-line with the concept of Least Privilege. The alternative would be to grant these six users full DBA access, but this would give them more privileges than required.

Recommendation 7 - Concur
Audit Trails and Warning Banner: Due to the SaaS provision of this system, certain configurations are beyond the control of DHS. Although the Oracle Hardening guide is not strictly adhered to, there are other tracking capabilities built into the application to allow auditing. Additionally, although the proper warning banner is not provided when logging on locally to the server, the proper DHS warning and privacy banners are provided for all users and candidates accessing the system. We were aware of these issues, but the application provider was not willing to change the settings because it would cause undue burden on the application's operating capability. Due to the fact that the TALENTLink system is being decommissioned and will be shut-down on 26 June 2010, we do not recommend the creation of a POA&M.

Appendix B
Management Comments to the Draft Report



JBoss Vulnerability: This vulnerability was identified prior to the OIG scan; however, a new build was required and not all zones received the new build prior to the scan. The vulnerability has since been remediated in all zones.

Recommendation 8 - Concur
Although we agree with the intent of the recommendation, DHS policy does not support the performance or security testing on another agency's IT systems. Based on DHS policy, the connection is to be well-documented with emphasis on the responsibilities of the two organizations including maintaining valid ATO, incident reporting, training and awareness, etc. OCHCO will include specific language in future Memoranda of Agreement/Understanding to document mutual responsibility and roles for security systems.

Recommendation 9 - Concur
The HRIT systems cited in the report are considered External Information Systems (EIS). These systems are managed by another government agency and are provided as a paid service for DHS use. The responsibility for Certification and Accreditation (C&A) of these systems is solely that of the host government agency. OCHCO will strengthen the Memorandum of Agreements/Understanding between the other government agencies to clearly delineate the responsibility for the systems to be squarely on the host government agency and that results are available to OCHCO.

Recommendation 10 - Concur
The HRIT systems cited in the report are considered EIS. These systems are managed by another government agency and are provided as a paid service for DHS use. The responsibility for security and management of these systems is solely that of the host government agency. The POA&M deficiencies noted in this report are not DHS specific, and OPM has made significant progress in the closure of over 100 POA&M items noted during prior year assessments of the EHRI systems.

Recommendation 11 - Concur
WebTA is currently being recorded in the OCIO inventory as an EIS. The system is managed by the U.S. Department of Agriculture (USDA) as part of their mandate to be a provider of this type of service for other government agencies. The responsibility for security and management of this system is clearly delineated as a USDA responsibility. However, DHS must decide to accept the NFC line of code where NFC would then own the C&A responsibility or DHS must own the system and accept the C&A responsibility. HCBS staff is currently working this issue with OCIO.

Thank you for the opportunity to work with your staff on this Audit. Should you have any questions, please call me at (202) 357-8151, or your staff may contact Vince Micone, Chief of Staff, at (202) 357-8408.

cc: Chief Information Officer

Appendix C
Major Contributors to this Report

Information Security Audit Division

Edward Coleman, Director
Chiu-Tong Tsang, Director
Mike Horton, Information Technology Officer
Aaron Zappone, Team Lead
Amanda Strickler, Information Technology Specialist
Michael Kim, Information Technology Auditor
Nazia Khan, Information Technology Specialist

Beverly Dale, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Deputy Under Secretary for Management
Chief Human Capital Officer
Chief Information Officer
Chief Information Security Officer
Director, Compliance and Technology Information Security Office
Deputy Director, Compliance and Technology Information Security Office
Information System Security Manger, ITSO, Headquarters Services Division
Audit Liaison, OCIO
Director, GAO/OIG Liaison Office

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.