Audit Report

OIG-19-006

FINANCIAL MANAGEMENT

Report on the Enterprise Business Solutions' Description of its HRConnect Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period September 1, 2017, to July 31, 2018

October 30, 2018

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 30, 2018

MEMORANDUM FOR NICOLAOS B. TOTTEN
ASSOCIATE CHIEF INFORMATION OFFICER (ACTING)
HRCONNECT
ENTERPRISE BUSINESS SOLUTIONS

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Report on the Enterprise Business Solutions' Description of its HRConnect Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period September 1, 2017, to July 31, 2018

I am pleased to transmit the attached subject report. Under a contract monitored by our office, RMA Associates, LLC (RMA), a certified independent public accounting firm, examined the Enterprise Business Solutions (EBS) description of controls for processing user entities' human resource transactions in its HRConnect system; and the suitability of the design and operating effectiveness of these controls. This report includes management's description of EBS' system, management's written assertion, and RMA's independent service auditor's report. The contract required that the examination be performed in accordance with generally accepted government auditing standards and the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements Number 18, *Attestation Standards: Clarification and Recodification*.

In its examination, RMA found, in all material respects:

- the description fairly presents the HRConnect system that was designed and implemented throughout the period September 1, 2017, to July 31, 2018;

- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period September 1, 2017, to July 31, 2018, and subservice organizations and user entities applied the complementary user entity controls assumed in the design of EBS' controls throughout the period September 1, 2017, to July 31, 2018; and

- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2017, to July 31, 2018, if complementary subservice organizations and user entity controls assumed in the design of EBS' controls operated effectively throughout the period September 1, 2017, to July 31, 2018.

In connection with the contract, we reviewed RMA's report and related documentation and inquired of its representatives. Our review, as differentiated from an examination in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on EBS' description of controls, the suitability of the design of these controls and the operating effectiveness of controls tested. RMA is responsible for the attached independent service auditor's report dated October 30, 2018, and the conclusions expressed therein. However, our review disclosed no instances where RMA did not comply, in all material respects, with generally accepted government auditing standards.

Should you have any questions, please contact me at (202) 927-0009, or a member of your staff may contact Mark S. Levitt, Manager, Financial Audit, at (202) 927-5076.

Attachment

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Department of the Treasury
Enterprise Business Solutions

Report on Department of the Treasury, Enterprise Business Solutions' Description of Its HRConnect System and on the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period
September 1, 2017 to July 31, 2018

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Table of Contents

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

I. INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY RMA ASSOCIATES, LLC

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Independent Service Auditor's Report

To: Inspector General,
Department of the Treasury
Acting Associate CIO,
Enterprise Business Solutions

Scope

We have examined Department of the Treasury, Enterprise Business Solutions' (EBS) description of its HRConnect system entitled "Description of Controls Provided by Enterprise Business Solutions" for processing user entities' human resource transactions throughout the period September 1, 2017 to July 31, 2018, (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Management Assertions Provided by Enterprise Business Solutions" (assertion). The controls and control objectives included in the description are those that management of EBS believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the HRConnect system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, "Other Information Provided by Enterprise Business Solutions" is presented by management of EBS to provide additional information and is not a part of EBS' description of its HRConnect system, made available to user entities during the period September 1, 2017, to July 31, 2018. Information about EBS' business continuity planning and management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description of HRConnect system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the HRConnect system and, accordingly, we express no opinion on it.

EBS uses two subservice organizations identified in Section III and IV to perform hosting services: Memphis Data Center (MDC) and National Finance Center (NFC). The description includes only the control objectives and related controls of EBS and excludes the control objectives and related controls of the MDC and NFC. The description also indicates that certain control objectives specified by EBS can be achieved only if complementary subservice organization controls assumed in the design of EBS' controls are suitably designed and operating effectively, along with the related controls at EBS. Our examination did not extend to controls of MDC or NFC, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

The description indicates certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of EBS' controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities
In Section II, EBS provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. EBS is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and applicable Government Auditing Standards issued by the Comptroller General of the United States. Those standards require we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period September 1, 2017, to July 31, 2018. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented, and the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in EBS' assertion:

1. The description fairly presents the HRConnect system that was designed and implemented throughout the period September 1, 2017 to July 31, 2018.
2. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period September 1, 2017 to July 31, 2018, and the subservice organizations and user entities applied the complementary user entity controls assumed in the design of EBS' controls throughout the period September 1, 2017 to July 31, 2018.
3. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2017 to July 31, 2018, if complementary subservice organizations and user entity controls assumed in the design of EBS' controls operated effectively throughout the period September 1, 2017 to July 31, 2018.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of EBS, user entities of EBS' HRConnect system during some or all of the period September 1, 2017 to July 31, 2018, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

RMA Associates

Arlington, VA
October 30, 2018

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

II. MANAGEMENT ASSERTIONS PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Nicolaos B. Totten
Acting Associate Chief Information Officer
Enterprise Business Solutions

October 30, 2018

We have prepared the description of Enterprise Business Solutions' HRConnect System entitled "Description of Controls Provided by Enterprise Business Solutions" for Treasury's enterprise human resources system processing user entities' transactions throughout the period September 1, 2017 to July 31, 2018 (description) for user entities of the system during some or all of the period September 1, 2017 to July 31, 2018, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description indicates certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Enterprise Business Solutions' controls are suitably designed and operating effectively, along with related controls at the service organizations. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the HRConnect system made available to user entities of the system during some or all of the period September 1, 2017 to July 31, 2018, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    i. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

        (1) The types of services provided, including, as appropriate, the classes of transactions processed;

        (2) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;

(3) The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

(4) How the system captures and addresses significant events and conditions other than transactions;

(5) The process used to prepare reports and other information for user entities;

(6) Services performed by subservice organizations, if any, including whether the inclusive method or the carve-out method has been used in relation to them;

(7) The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organizations' controls; and

(8) Other aspects of our control environment, risk assessment process, information, and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. Includes relevant details of changes to service organizations' system during the period covered by the description; and

iii. Does not omit or distort information relevant to service organizations' system, while acknowledging the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors; and may therefore, not include every aspect of the HRConnect System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period September 1, 2017 to July 31, 2018, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of EBS' controls throughout the period September 1, 2017 to July 31, 2018. The criteria we used in making this assertion were that:

i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of service organizations;

ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. The controls were consistently applied, as designed, assuming manual controls were applied by individuals, who have the appropriate competence and authority.

Nicolaos B. Totten
Acting Associate Chief Information Officer
Enterprise Business Solutions
Department of the Treasury

Nicolaos B. Totten Digitally signed by Nicolaos B. Totten
Date: 2018.10.30 09:32:03 -04'00'

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

III. DESCRIPTION OF CONTROLS PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

OVERVIEW OF OPERATIONS

This examination only covers the products and services provided by the Enterprise Business Solutions (EBS) relating to the HRConnect system. In 2005, the Office of Personnel Management awarded EBS the Human Resources Line of Business (HRLOB) status, a certification that identifies its software products and services as a "best practice" within the federal sector. As an HRLOB Shared Services Provider, the HRConnect System is used by all Treasury bureaus and several other government agencies (over 34 entities) with over 180,000 employees and contractors in total.

HRConnect System is Treasury's enterprise human resources system. HRConnect System is based on a combination of (a) web-based solution built on PeopleSoft commercial-off-the-shelf (COTS) software, and (b) Software as a Service (SaaS) platforms (e.g. Talent Management). HRConnect System transforms core back-office Human Resources (HR) functions, moving them from a processing-centric capability to a strategic-centric capability enabled through its commercial software underpinning. Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.

HRConnect System supports the common HRLOB processes and provides core HR functionality that is interoperable, portable, and scalable. This shared solution provides automated systems that are configurable to the individual organizations' needs while providing a single solution across the Department and federal landscape. HRConnect Services' core functions include Personnel Action Processing, Managing Payroll Interface, ePerformance, Position Management, Job Code, Recruit Request, Manager Self Service, Employee Self Service, Federal Activities Inventory Reform (FAIR) Act, Personal Identity Verification (PIV) Data Synchronization (PDS) and Contingent Worker, and SEC (Separating Employee Clearance). By enabling the retirement of legacy systems and automating and streamlining many aspects of human resources, HRConnect System facilitates increased efficiency and overall productivity for its customers. The mission of HRConnect System is to address common operational needs and imperatives of the Department of the Treasury and other Federal agencies in an efficient and innovative manner through shared, scalable, best-practices-based online solutions.

The HRConnect Products and Services Chart, Figure 1, appears below.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

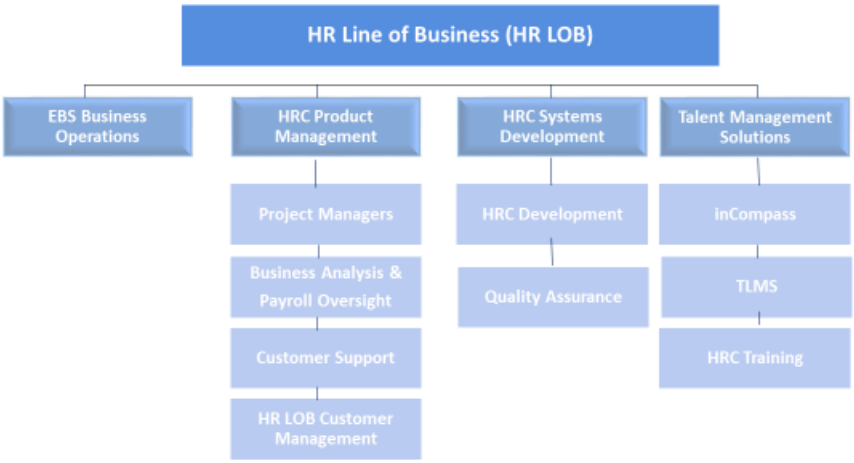

Figure 1: HRConnect Products and Services

HRConnect

The HRConnect system is an enterprise web-based HR system, built on PeopleSoft commercial off-the-shelf software, and is the foundation of the Treasury Shared Service Center's comprehensive suite of solutions. HRConnect transforms core back-office HR functions, moving them from processing-centric paper or legacy systems to a strategic-centric capability enabled through its commercial software underpinning.

Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers, employees, and HR professionals. HRConnect features/functionality include:

List of HRConnect Products and Services:

HRConnect System Features/Functionality	
Automated Password Management	Treasury HRConnect walks new users through the initial registration process, assigning a User ID and temporary password. Forgotten IDs/Passwords, as well as Need to Change Passwords, are also managed in the same secure environment. Help Desk intervention is not required, except for unlocking user accounts.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

HRConnect System Features/Functionality	
Manager, Employee and HR Self Service	Personnel Action Requests (the electronic equivalent of an SF-52) may be initiated online by Managers (and/or their Proxies or Detail Managers) using Manager Self Service. HR staff can process or initiate a full suite of Office of Personnel Management (OPM)-approved transactions (in 55 different action/reason categories) in HRConnect. A Mass Update Module feature is also available to HR to easily process many similar requests with one transaction (realignments, reassignments, etc.). Employees may initiate 9 actions and 19 updates to personal information, including address, phone number, and emergency contact information as well as the ability to request to retire or resign. In addition, users may view personal information, benefits, leave balances, and salary, performance and award history.
Personnel Action Requests (PARs)	PARs may be initiated by Managers, their Proxies, Detail Managers, and HR specialists. HR staff can process a full suite of OPM-approved transactions (over 150 PAR actions) in HRConnect. A Mass Update Module feature is also available to easily process many similar requests with one transaction (realignments, reassignments, etc.).
Payroll Interface and Error Correction	Treasury HRConnect features a robust daily bi-directional interface transmitting personnel, position, and payroll information to the National Finance Center (NFC), Treasury's payroll partner. The reverse interface provides all applied actions, historical corrections, and NFC-generated automatic actions (within-grade increases, etc.) back to Treasury HR System (HRConnect). This interface allows for error correction (SINQ's) directly in Treasury HRConnect and delivers a comprehensive match solution to keep data synchronized.
Payroll Processing	Treasury HRLOB partners with the NFC to perform all the payroll related processes as well as other services normally associated with payroll.
Benefits Administration	Treasury HRLOB's HR processing partner, Fiscal Service Administrative Resource Center, provides staff to support the administration of benefits (retirement, life insurance, health insurance, TSP, LTCIP, FSA, retirement annuity calculations, EAP). This is a separate service Treasury customer can request. Additionally, HRConnect provides convenient access to a number of helpful links to a variety of information including National Finance center Employee Personal Page, tax calculator, salary tables, TSP information, safety and health programs, and more.
Interfaces to Agency/Bureau and other service provider systems	Treasury HRConnect provides data feeds to multiple Agency/Bureau systems, including data warehouses, Learning Management systems, and other service providers. These interfaces can be accomplished through a variety of technical processes.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

HRConnect System Features/Functionality	
Workflow and Worklists	Managers and HR specialists are able to access actions directed to them online for authorization or approval using workflow and worklists. Personnel and other actions are moved automatically through a configurable workflow that includes management authorizations and HR approvals. A sophisticated set of routing rules can be invoked to direct actions by type or location to HR specialists in that category of action (e.g., Suspensions to ER specialists).
Position Description Library	Standard, authorized position descriptions (PD's) are available online for HR and managers, replacing the need to establish new position descriptions and undergo classification each time a new position is required.
Position Management	Treasury HRConnect provides the ability to manage workforce through position creation, allocation, budgeting, obligation, and incumbency tracking, including a Position Wizard.
Position Budget Management	Position Budget Management (PBM) allows a budgeting office to designate the distinct account code or codes to which the payroll expenses for a specific position will be charged. This function prevents the use of positions for which no account code has been assigned and automates the assignment of new codes as well as the removal of inactivated codes. Automated workflow and system-generated notifications, as well as standard reports and the inclusion of position budget data in the Workforce Analytics reporting system, enable budget analysts to monitor the position budget status of their assigned organizational units and to take action as needed.
Mass Processing	At times, managers may wish to initiate mass actions that impact a group of employees. Manager Self Service efficiently handles mass awards and mass realignments.
Payroll Documents	HR specialists have the ability to initiate 30 different payroll documents (e.g., Federal, state and local taxes, allotments, health insurance, direct deposits, and health benefits, including several non-Federal documents) directly in HRConnect and have them transmitted to NFC.
Emergency Contacts	Employees can input an extensive list of emergency contacts. Information includes the contact name, address, phone number(s), and relationship to the employee. This information can be accessed and updated at any time and reports are available to Managers and HR professionals.
Awards Administration	Managers and HR may initiate many types of awards (on-the-spot, cash, time-off, etc.) for direct-reporting employees as well as others in the organization. Bureaus can elect to require optional data fields, e.g., accounting code. Administrators have the ability to specify award codes and limits applicable to their agency that are available in a list for managers to initiate and select. This feature includes the ability to initiate mass award actions for many employees.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

HRConnect System Features/Functionality	
Separating Employee Clearance	Treasury HRConnect allows online management of the process of clearing an employee who is separating (e.g., securing issued equipment, security passes, credentials, etc.).
Drug Test Tracking	Treasury HRConnect provides a way to track drug testing information.
Employee and Labor Relations, and Third-Party Case Tracking	Treasury HRConnect provides for tracking of disciplinary cases, grievance cases, and third party (arbitration, etc.) cases. Also allows for tracking negotiation processes between bargaining units and management.
Financial Disclosure Tracking and Reporting	Treasury HRConnect provides the ability to track employees required to submit Forms 278 and 450 financial disclosure forms.
FAIR Act Reporting	Treasury HRConnect provides for the creation and submission of OMB-compliant FAIR Act reports.
SF-50's	Treasury HRConnect provides the capability for employees and HR professionals to access, view and print SF-50's online, including required email notification to employees of the availability of their SF-50's.
Automated Email Notifications	Treasury HRConnect automatically sends users notification and reminder emails for NTE dates, SF-50's, worklist items, password expiration, etc.
Continuity of Operations Tracking	Treasury HRConnect provides managers the capability of entering and maintaining Continuity of Operations (COOP) group assignments for their employees and the skill sets required for bureau/agency continuation of operations.
System Security	Treasury HRLOB's foundational approach to information security for all IT systems developed and managed by this office is a Defense-In-Depth principle implemented as a layered solution. In short, there are multiple defense strategies for multiple targets or initiatives.
Attachments	HRConnect provides the ability for Employees, Managers/Proxies, and HR to attach documentation to actions. Attachment functionality allows approving authorities, reviewers, and processors to easily access and review supporting documentation in order to take immediate action, as necessary. Attachments are available in the following areas: personnel actions initiated by HR or Managers; employee updates (e.g., name change); recruit requests; Employee/Labor Relations cases; Health Benefit forms; dependent information; and Separation and Home Leave.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

HRConnect Services/Support	
Tier 1 Help Desk Support	Treasury HRLOB partners with the Administrative Resource Center (ARC) to offer Tier 1 Help Desk support. If a customer does not utilize ARC, then the customer is responsible for Tier 1 Help Desk support.
Tier 2 and Tier 3 Help Desk Support	Treasury HRLOB's second and third tier Help Desk support to supplement an organization's first tier.
Business Process Analysis	Treasury HRConnect' s specialists assess the customers' current processes and assist in developing future state processes and a plan for implementation. This is based on an analysis done with the organization to ensure that the processes are in alignment with and best utilize the HRConnect technologies
Organization Change Management	Treasury HRLOB's Change Management consultants provide guidance, lessons learned, best practices, and variety of processes and techniques to obtain stakeholders' support for change. This is done with the customer to ensure that executive sponsorship and change agents are identified early in the process to ensure success.
System Training	Treasury HRLOB conducts a 3-day course which provides new HR Specialists with hands-on experience on initiating, routing, and processing HR actions. It reviews the common interfaces and provides understanding of how to process, job requisitions; personnel actions requests; SINQs; cancellation and corrections; and workflow requests. In addition to classroom training, the Treasury HRLOB Training Solutions Team is also able to provide webinars, user guides, and more. Additionally, there is an established Customer-based Community of Practice group which meets regularly to educate customers on the various features and functions available.

Table 1: List of Products and Services

Relevant Aspects of the Control Environment, Risk Assessment, and Monitoring

Control Environment

The control environment is the foundation for all other components of internal control. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. EBS has established and maintained an environment throughout the organization that sets a positive attitude toward internal control. Through its management, EBS has demonstrated a commitment to integrity and ethical values and a commitment to a strong internal control system. EBS has established an organizational structure, assigned responsibility, and delegated authority to achieve its objectives. EBS is committed to recruit, develop, and keep competent individuals. EBS evaluates performance and holds individuals accountable for their internal control responsibilities.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

EBS is one of Treasury's Government Shared Services and HRConnect is one of the shared offerings. The mission of EBS is "To address common operational needs and imperatives of the US Treasury and other Federal agencies in an efficient and innovative manner through shared, scalable, best-practices-based online solutions."

HRConnect employees and contractors are responsible for providing HRConnect system operation and maintenance, which includes the governance and development of changes to the system such as mandatory and regulatory changes, change requests and defect management. Each HRConnect employee has a written position description. All HRConnect employees and contractors with system access receive background investigations and clearance in accordance with Treasury policy. All HRConnect employees and contractors with system access receive mandatory annual training in ethics, privacy, and IT security. Additionally, managers work directly with employees to implement development plans tailored to the employees' needs in work-related topics such as project management, analysis, payroll processing, OPM HR standards, and PeopleSoft Human Capital Management Solutions.

Federal employees follow the Standards of Ethical Conduct for Employees of the Executive Branch that cover the 14 general principles of ethical conduct Codified in 5 C.F.R. Part 2635. Annual privacy training is required by FAR Subpart 24.3 that addresses the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. In addition, all users of information systems must receive awareness training, as required by the Federal Information Security Modernization Act of 2014 (FISMA).

All HRConnect employees receive an annual written performance evaluation. These reviews are based on goals and objectives that are established and reviewed during meetings between the employee and the employee's supervisor. Completed appraisals are reviewed by senior management and become part of the employee's official personnel file.

Risk Assessment

EBS has a risk assessment process to identify and manage risks that could affect its ability to provide services to its customers. The process requires team members, project managers, and the management team to identify risks and issues in their areas of responsibility and to implement appropriate measures and controls to manage these risks. Risks are updated continuously and escalated based on their severity. Additionally, the risk log is analyzed and updated by the Applications Portfolio Management team and high/critical items are brought for review every two weeks by the entire management team.

Monitoring

Monitoring internal control is a dynamic process that has to be adapted continually to manage changing risks. Monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal control

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

monitoring assesses the evaluation of the effectiveness of controls over time and promptly resolves the findings of audits and other reviews. EBS has established monitoring activities and reacts to events timely with corrective actions. Corrective actions are a necessary complement to control activities in order to achieve objectives.

HRConnect management and supervisory personnel monitor the quality of performance as a normal part of their activities. Management and supervisory personnel inquire of staff and/or review data to ensure the system operates within an effective internal control environment. An example of a key monitoring control is capturing key performance indicators in the monthly Performance Management Review (PMR) report.

EBS uses Plan of Action and Milestones (POA&M) as a tool to document the planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The purpose of HRConnect' s POA&M is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in its programs and systems. POA&M delineates resources required to accomplish the elements of the plan, any milestones in meeting the task and scheduled completion dates for the milestones. At a minimum quarterly, EBS reviews POA&M items for consistency with EBS risk management strategy and organization-wide priorities for risk response actions.

Information and Communication

HRConnect offers interoperable, portable and scalable HR/payroll solutions across the Federal space. HR Connect core functions include: Personnel Action Processing, Payroll Administration, Benefits Administration, Talent Acquisition, Onboarding, Treasury Learning Management, Integrated Talent Management, Employee and Manager Self Service Portal, Time and Attendance, and HR transaction processing.

EBS uses information to support its internal control system. Information and communication are vital for EBS to achieve its control objectives. EBS has implemented an information security monitoring that maintains ongoing awareness of information security, vulnerabilities, and threats to support EBS risk management decisions.

HRConnect Core is based on the PeopleSoft application. The components are PeopleSoft 9.2, Tools 8.55, Oracle 12C database, WebLogic Web/App servers and Solaris 11 running on SPARC servers.

EBS has established an effective control environment, management assesses the risks facing HRConnect as it seeks to achieve its control objectives. EBS applies Risk Management Framework (RMF) to HRConnect which includes conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. EBS uses Treasury FISMA Inventory Management

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

System (TFIMS) to document this process. An initial National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 compliant risk assessment was completed as part of the Security Assessment and Authorization (SA&A). The next full formal Risk Assessment is planned for the Annual Assessment due June 2019 or the next full SA&A in September 2019. The plan provides the basis for developing appropriate risk responses. EBS assesses the risks to HRConnect from both external and internal sources. HRConnect follows Continuous Monitoring actions throughout the year in a variety of FISMA-compliant actions to review system changes for security impacts and risks. EBS has clearly defined HRConncet control objectives to enable the identification of risks and define risk tolerances. In the HRConnect, EBS identifies and analyzes risks related to achieving the defined objectives. In addition, EBS analyzes risk to be able to respond to significant changes that could impact the internal control system.

HRConnect System Security Plan (SSP) provides a summary of the security requirements for the HRConnect system and describes the security controls in place or planned for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. The SSP includes security-related documents for the information system such as a Federal Information Processing Standards (FIPS) 199 Security Categorization, risk assessment, POA&Ms, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, and security configuration requirements.

EBS controls the HRConnect SSP by placing the plan in the TFIMS. TFIMS provides functionality to collect and manage data required by FISMA. TFIMS features include:

- Ability to track POA&Ms, artifacts, and contacts;
- Permission controlled access to systems; and
- Search by keyword and other parameters.

Systems and Interfaces

EBS uses the following systems and interfaces to provide HRConnect System to Federal agencies.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

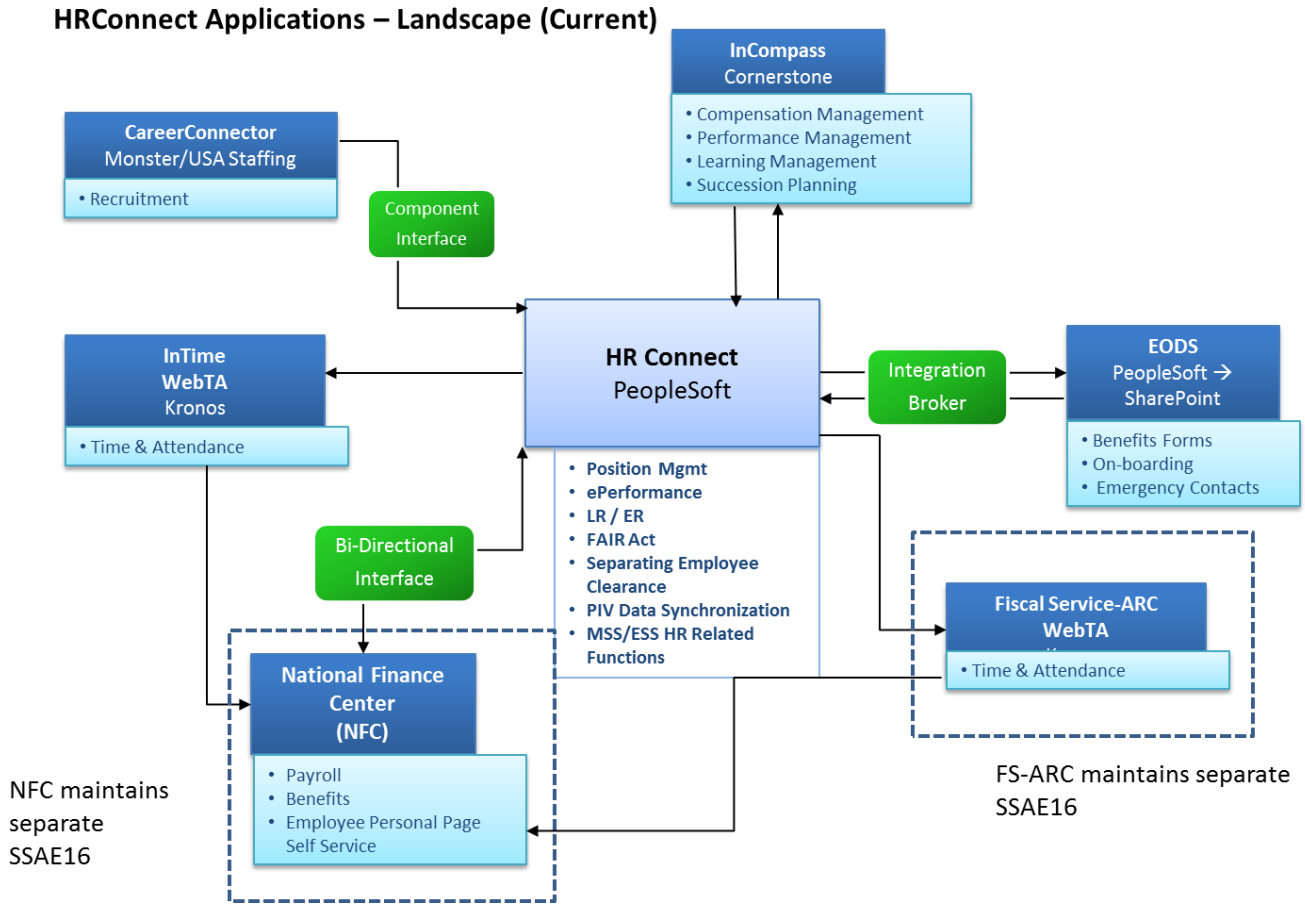

Figure 2: HRConnect Applications – Landscape (Current)

Note: HRConnect does not automatically feed WebTA. This is done manually. Also, CareerConnector and Entrance on Duty System (EOD) systems are not included in this examination.

HRConnect

HRConnect Core supports the common HRLOB processes and provides core HR functionality that is interoperable, portable, and scalable. This shared solution provides automated systems that are configurable to the individual organizations' needs while providing a single solution across the Department and Federal landscape. HRConnect's functions include employee self-service, manager self-service, HR processing, and bi-directional payroll interface. The data that are tracked include, but are not limited to:

- Employee and Contractor personal information including data such as Name, Address, Gender, Disability, Social Security Number (SSN), Salary, etc.;

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- Employee skills, education, and certificates;
- Personal Action Processing and awards that managers can manage;
- Workflow capability that enables HR and Budget office to control position management
- FAIR Act;
- Separation Employee Clearance;
- Position-related actions that HR Specialists can approve and initiate; and
- Payroll documents and benefits that HR Specialists can manage.

There is a payroll interface that transmits the payroll data to the NFC. Once customers implement HRConnect, they are able to retire legacy systems and automate and streamline many aspects of human resources. HRConnect facilitates increased efficiency and overall productivity for its customers. HRConnect Core is based on the PeopleSoft application.

The HRConnect application, a FISMA High system, has full disaster recovery capabilities and implements continuous monitoring for FISMA compliance. System health and the availability are monitored by Oracle Enterprise Manager (OEM) and Foglight. These monitoring tools send alerts before the occurrence of an issue by using thresholds. The Technical Architecture team also monitors the system using cronjobs to alert any issues. The Security team uses Splunk for event aggregation and monitoring, and other tools listed below to check all layers of the system.

Security monitoring tools include:

- Nessus – vulnerability scanner (scans any system with an Internet Protocol (IP) address and can recognize multiple systems) to detect vulnerabilities at the operating system and IP layer;
- DBprotect – vulnerability scanner for databases;
- WebInspect – vulnerability scanner for web applications and web interfaces;
- Splunk – collects logs from multiple types of IT systems for correlation and monitoring system activities with alerts; also used for log retention;
- TripWire – used to monitor files on systems for file integrity;
- F-PROT – antivirus for file border server files; and
- Symantec ICAP – antivirus for end-user file attachment uploads.

inCompass

inCompass is EBS' integrated talent management platform. The inCompass software product is a single set of data that supports five areas of Human Capital Management. Each area is represented by a module within inCompass. The five modules are Learning Management, Performance Management, Workforce/Succession Planning, Compensation Management, and Connect - Social Media. inCompass supports the ability for an end user to develop concrete performance goals, uses competency and skill assessments to identify skill gaps, and encourages career development through learning activities and targeted manager feedback. Data integration between inCompass and HRConnect further ensures accuracy and efficiency by removing the need for manual entry of

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

data into the system for HRConnect customers. inCompass may be purchased independently of the HRConnect product suite but is most effective when interconnected with other core HR systems.

The inCompass program sits on the SaaS application Cornerstone OnDemand (CSOD). EBS has worked with CSOD to design inCompass to meet unique Federal needs such as the Federal Risk and Authorization Management Program (FedRAMP) security requirements, and OPM Enterprise Human Resource Integration (EHRI) data feed requirements. CSOD is in use worldwide and across multiple industries, which provides EBS extensive flexibility to configure inCompass to meet customers' needs as they grow and evolve. inCompass offers over 200 standard reports coupled with drag and drop custom reporting capability that enhances each agency's ability to analyze its data on the fly.

No SSNs or birthdates are ever stored or processed within the inCompass environment.

Personnel identity and other information described in the Interconnection Security Agreement (ISA) is pushed from the HRConnect to the inCompass Secure File Transfer Protocol (SFTP) Server:

1. A Data Load Wizard extracts information from the data files and updates the inCompass databases.
2. The inCompass application calls data from the database for presentation to the user, based on the module the user is accessing.
3. The inCompass user enters information to complete forms that are passed by the application to the respective database.
4. Data is extracted from inCompass databases to the inCompass SFTP server.
5. HRConnect Border Server pulls data from the inCompass SFTP via a scheduled data feed.

Inbound encrypted SFTP connections are initiated by the Treasury HRConnect Border Server to the inCompass SFTP server for the purpose of regularly scheduled data transfers. The HRConnect Border Server always initiates this connection and both pushes and pulls data feeds to the inCompass SFTP server. This connection is intended for bulk data transfers, to transfer updated records, in support of the inCompass modules. The data feed is encrypted using FIPS 140-2 validated cryptographic modules. Additional information about the contents of the data feeds is located in the ISA between the Treasury and inCompass. End users and administrators access their inCompass portals via web browsers. All configuration and other portal administration functions are performed through the users' web browser. Once authenticated, users can access their portal and interact with the modules as desired. Cornerstone provides the delivery of the application and module content to inCompass users through Akamai servers. The entire session over the Internet is encrypted using FIPS 140-2 validated cryptographic modules. The inCompass system also sends users email notifications based on triggers and parameters defined by each customer. No Personal Identifiable Information (PII) is allowed to be sent via unencrypted email.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Cornerstone employees periodically connect to the inCompass environment to implement approved Change Requests (CRs), apply patches, run vulnerability scans, troubleshoot errors, and perform routine maintenance of inCompass assets. All CSOD connections are over a multi-factor Virtual Private Network (VPN) session from the CSOD corporate network.

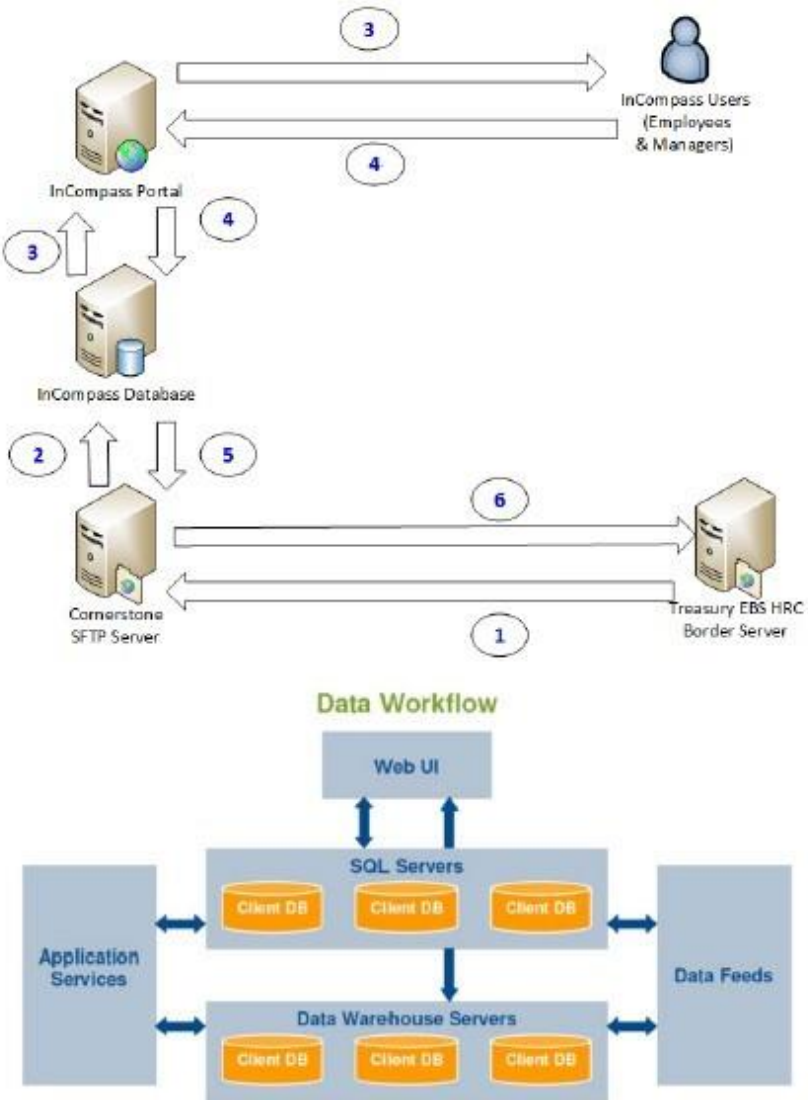

Figure 3: HRConnect Workflow

InTime

EBS hosts WebTA 4.2 from Kronos as its time and attendance solution for the Department of Labor (DOL). WebTA is a current off the shelf web application that can be deployed over various platforms. Treasury's InTime solution resides on multiple web/app servers running on Tomcat and

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Linux platforms with an Oracle database backend. Currently, there are two web/app servers with the ability to scale to as many more as needed to support demand. The web app servers are served by a pair of F5 load balancers and a pair of fault tolerant firewalls.

InTime data is backed up every night using a disk-based backup solution. Copies of the backup are placed on removable media and regularly rotated offsite to a protected and geographically remote storage facility. This provides the best solution in terms of speed and efficiency of disk-based backup strategies with the portability of media-based backup strategies.

Talent Learning Management System (TLMS)

SuccessFactors has developed and maintained a Contingency Plan and an Incident Response Plan for the San Francisco Financial Center (SFC). These plans describe the steps to take in the event of an unexpected disruption or a security-related anomaly. The plans are tested annually and reviewed/updated after the exercise is completed and analyzed. The tests also serve as refresher training for the personnel who participate in the activities defined in each plan.

Backup servers use Symantec NetBackup and a Data Domain server performs data de-duplication, encryption, and replication over the wire to a second Data Domain server at the alternate storage site in Chandler, AZ, 2,300 miles from the primary site. SuccessFactors uses site-to-site replication and therefore does not utilize removable media. Some agencies are required to send certain statistical HR information to the OPM periodically. For that purpose, the SFC uses a connector that transmits the HR information to OPM using Secure Shell (SSH).

Site-to-site communication between the SFC in the Ashburn data center and the alternate site in Arizona is via a Multi-Protocol Label Shipping (MPLS) cloud. If the MPLS cloud is down, site-to-site traffic are sent through a backup route consisting of Internet Protocol Security (IPSec) VPN tunnels.

At the Verizon data center, the network is segmented with Virtual Local Area Networks (VLANs) to provide separation between tiers in combination with a firewall. Packets are switched at the data link layer (OSI layer 2) within VLANs and are routed at the network layer (OSI layer 3) through the firewall to provide a managed/controlled interface to govern data traffic flows between VLANs.

Complementary Subservice Organization Controls (CSOCs)

EBS' controls relating to the HRConnect system cover only a portion of the overall internal control structure of each user entity of EBS. It is not feasible for the control objectives relating to EBS services to be solely achieved by EBS. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with EBS' controls and related testing detailed in Section IV of this report, considering the complementary subservice organization controls expected to be implemented at the subservice organization as described below.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Memphis Data Center (MDC)

The IRS MDC located in Memphis, TN, is the primary data center for production services for EBS systems. The MDC serves approximately 3,000 general users. The MDC includes application, file/print, data backups, communication, utility and management servers, network cabling, routers, switches, and other communications equipment required to support network connectivity. InTime uses database replication between its primary site in Reston, Virginia and its alternate site in Denver, Colorado.

National Finance Center

HRConnect features a daily bi-directional interface transmitting personnel, position, and certain payroll information to the NFC, Treasury's payroll provider. The reverse interface provides all applied actions and NFC-generated automatic actions (within-grade increases, etc.) back to HRConnect.

	Complementary Subservice Organization Control	Related Control Objective
	MDC	
1	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
	NFC	
2	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
3	Responsible for assuring that only valid payroll/personnel transactions are accepted, processed completely and accurately, and reported to customer agencies:	CO 10
4	Responsible for assuring that master data is complete, accurate, and valid:	CO 10

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Complementary User Entity Controls (CUECs)

EBS' controls related to its system processing user entities' human resource transactions cover only a portion of overall internal control for each customer of EBS. It is not feasible for the control objectives related to EBS' services to be achieved solely by EBS. Therefore, each customer's internal control over financial reporting should be evaluated in conjunction with EBS' controls related tests and results described in Section IV of this report, considering the related CUECs as described below, where applicable. In order for customers to rely on the controls reported on herein, each customer must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

Control Objective 4: Access to Computerized Applications

User entity auditors should determine whether user entities have established controls to provide reasonable assurance to properly:

1. Grant access to the systems to users who have been vetted by their organization's security requirements;
2. Provide appropriate levels of privileged user access to the systems to users who have a bona fide need and have met their organization's security requirements; and
3. Assign security roles to users based on their role in the system (e.g. personnel specialists would hold the HR Specialist role vs. a manager who would hold the manager role in HRConnect).

Control Objective 9: Secure Interface Processes

User entity auditors should determine whether user entities have established controls to provide reasonable assurance that:

1. The User Entity's technical contact tests connectivity from the User Entity's border server to the EBS border server using SSH and SFTP.
2. Recommended but not required: The User Entity's technical contact places the User Entity's border server public key on the EBS border server so that certificate-based authentication can take place.
3. The User Entity's technical contact tests file transfers (pushes and pulls) between the User Entity's border server and the EBS border server.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Control Objective 10: Subservice Organizations

User entity auditors should determine whether user entities have established controls to provide reasonable assurance that:

1. SINQ errors, HCUP Status, and mismatch cases are corrected to ensure transactions are processed.
2. The mismatch tables are reviewed and corrected.

Control Objectives and Related Controls

EBS has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in Section IV, "Control Objectives, Related Controls, And Tests of Operating Effectiveness," and are an integral component of HRConnect's description of its Enterprise Human Resources System.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

IV. CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTING

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Test of Control Environment Elements

In addition to the test of the operating effectiveness of specified controls described in this Section, our procedures included consideration and tests of elements of EBS' control environment, as described in Section III.

Such tests included inquiry of appropriate management, supervisory, and staff personnel; inspection of EBS' documents and records; and observation of EBS' activities and operations. The results of these tests regarding the control environment were considered in planning the nature, timing, and extent of our tests of the specified controls placed in operation, related to the control objectives described below.

Tests Performed	Test Descriptions
Inquiry	Inquired of relevant personnel with the knowledge and experience of the performance and application of the related control activity. This included in-person interviews, telephone calls, or e-mails.
Observation	Observed the relevant processes or procedures during fieldwork. Observation included walkthroughs; witnessing the performance of controls; or evidence of control performance with relevant personnel, systems, or locations, relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included documents; system configurations and settings; or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing items to supporting documents, system documentation, or processes.
Reperformance	Reperformance of calculations. This included an independent performance of the calculations that were originally performed as part of the EBS' internal control.

Control Objectives, Related Controls Placed in Operation, and Tests of Operating Effectiveness

This section presents the following information provided by EBS:

- The control objectives specified by the management of EBS; and
- The controls established and specified by EBS to achieve the specified control objectives.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Also, included in this section is the following information provided by RMA Associates, LLC (RMA):

- A description of the testing performed by RMA to determine whether EBS' controls were operating with sufficient effectiveness to achieve specified control objectives. RMA determined the nature, timing, and extent of testing performed.
- The results of RMA tests of operating effectiveness.

Security Management Controls

Control Objective 1: System Security Plan

Controls provide reasonable assurance that management has established, implemented, and monitored HRConnect system security plans.

Description of Controls

The Treasury Department is mandated to comply with Federal Information Security Modernization Act of 2014, Public Law 113–283 (December 18, 2014) which requires agencies to have effective information security controls over Information resources to support federal operations, assets and provide a mechanism for improved oversight of agency information security programs.

HRConnect SSP is the foundation of a security control structure and a reflection of EBS' commitment to addressing security risks. The SSP establishes a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

EBS has supplemented the Department level controls by implementing specific procedures and controls at the HRConnect applications. EBS has followed and documented Departmental Offices, EBS, and HRConnect specific security policies that have been made available to affected personnel, including HRConnect employees and contractors. These policies include system and application rules and expected user behaviors.

The HRConnect SSP provides an overview of the security requirements as it applies to HRConnect, and it describes the controls in place for meeting those requirements. The HRConnect SSP delineated responsibilities and expected the behavior of all individuals who access the system. The HRConnect SSPs are maintained by the HRConnect Cyber Security team and housed within the TFIMS.

EBS applied RMF to HRConnect which included conducting the activities of security categorization, security control selection and implementation, security control assessment,

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

information system authorization, and security control monitoring. EBS uses TFIMS to document this process.

The security plan establishes security categories for both information contained in HRConnect and the HRConnect application based on Federal Information Processing Standards Publication (FIPS Pub) 199: *Standards for Security Categorization of Federal Information and Information Systems.* EBS used the FIPS Pub 199 to determine the Security Categories risk level of high, moderate, or low. EBS selected the controls to implement based on FIPS Pub 200: *Minimum Security Requirements for Federal Information and Information Systems* and NIST Special Publication 800-53 Revision *4: Security and Privacy Controls for Federal Information Systems and Organizations*. An independent party performs SA&A at least annually to determine the extent to which the system's security controls are implemented correctly, operating as intended. The assessor evaluates management, operational, and technical controls. As a result of the SA&A process, findings are analyzed, and a POA&M is created for each control that has failed. When the SA&A is completed, the assessor issues the Security Assessment Reports (SARs). The SAR is performed annually on approximately one-third (1/3) of the security controls, which constitutes a Risk Assessment. The Authorizing Official inspects the SSP, SA&A, SAR, and POA&Ms to determine whether to Authorize to Operate (ATO) for HRConnect EBS maintains and updates SA&A documentation at least annually.

In accordance with the Department's Continuous Monitoring Strategy, a set of controls from NIST SP 800-53 Rev 4 are defined for system authorization testing annually. The test results are placed in TFIMS by June 30th of every year. HRConnect follows Continuous Monitoring actions throughout the year to review system changes for security impacts. These include monthly and ad-hoc security vulnerability assessment and security configuration across the system layers, security impact/risk assessments on system changes.

TFIMS provides a centralized system for the management artifacts that support assessments, documentation, and reporting on the status of IT security risk assessments and implementation of Federal and NIST standards. TFIMS helps manage and track POA&Ms to include creating, tracking, and closing, as well as automating system inventory and FISMA reporting capabilities. Sufficient evidence must be provided in order to close each POA&M. POA&Ms are utilized to identify any findings, deficiencies, or weaknesses noted in all types of reviews. EBS program management, via System Owner (SO), Information System Security Officer (ISSO), Information System Security Manager (ISSM) and CyberSecurity Team, monitor and track any findings identified in internal and external audits as POA&Ms.

Tests of Operating Effectiveness and Results of Testing

1. Inspected the SSP's key elements of a security management program and determined the SSP was adequately documented and properly approved.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

2. Inspected the Security Assessment & Authorization (SA&A) and determined the SA&A for HRConnect was conducted annually.
3. Inspected recent POA&Ms and determined the status of corrective actions was appropriately monitored.
4. Inspected corrective action plans and determined the solutions were appropriately considered.
5. Inspected a selection of corrective action plans and determined testing was performed, and monitoring was conducted after the implementation of corrective actions. **Exception noted**. Artifacts required for closure of two POA&Ms from a selection of ten were not provided.

No exceptions were noted, other than the exception listed in test 5.

Control Objective 2: Security Related Personnel Policies

Controls provide reasonable assurance that Security related personnel policies are established, implemented, and monitored, including hiring practices of background investigations, confidentiality agreements, termination, and transfer procedures, IT Cybersecurity Awareness training, and exit interviews, which encompass the returning of property, keys, and removal of logical and physical access.

Description of Controls

<u>On-Boarding and Off Boarding</u>

HRConnect inherits NIST SP 800-53 Rev 4 Personnel Security (PS-1) controls, e.g., background investigation from the Department of the Treasury Security Manual (Treasury Department Publication (TD P)) 15-71.

All Treasury EBS employees and users with access to Sensitive But Unclassified Information (SBU) data are restricted to those who have completed and favorably adjudicated background investigations. All approved users who require elevated privileges must complete the Treasury Shared Services Center access request forms, comply with all HRConnect Rules of Behavior and related requirements. Federal employees and contractors/subcontractors are required to have a completed and favorably adjudicated background investigation that is, at a minimum, compliant with Homeland Security Presidential Directive-12 ((HSPD-12) requirements. The HSPD-12 minimum investigation is a National Agency Check with Inquiries (NACI) or such higher-level investigation may be required by the risk level or sensitivity of the position. Individuals lacking Personnel Security approval, regardless of permission levels, will be denied access.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Employee exit procedures, including a Provisioning for Personnel (P4P) form, are completed for termination of access privileges and the return of property. EBS receives Personal Identity Verification (PIV) cards of terminated employees and deactivates their physical access privileges.

Training

EBS personnel are provided with and required to take IT Cybersecurity Awareness training, Ethics training, and Privacy Awareness training on an annual basis. EBS offers application specific training to HRConnect customers. Treasury employees and contractors are required to complete and sign a Rules of Behavior and confidentiality agreements prior to obtaining access to the Treasury network. New employees are required to complete the Cyber Security Awareness training and acknowledge the Departmental Offices Rules of Behavior agreement prior to obtaining access to the Treasury network. Security-related subject matters are regularly emailed to personnel and posted to the internal share drive.

Tests of Operating Effectiveness and Results of Testing

1. Inspected security-related emails and posts to the internal share drive and determined security-related subject matters were regularly emailed to personnel and posted to the internal share drive.
2. Inspected a selection of employee's and contractor's files and determined new employees received an onboarding package of information regarding internal security policies prior to their start date.
3. Inspected a selection of employee's and contractor's files and determined internal security policies (Rules of Behavior and Cybersecurity Awareness) and agreements were signed and dated, and the Security Awareness training was completed.
4. Inspected the Exit Procedures and determined the procedures agreed to management policy.
5. Inspected a selection of the terminated employees' and contractors' records and determined P4P forms were completed. **Exception noted**. There were no records of the return of a PIV card for one terminated employee/contractor out of a selection of ten.
6. Inspected a system-generated list of users that left EBS in the current year and determined IDs and passwords were removed or deactivated from HRConnect.
7. Inspected security awareness training policies and procedures and determined adequate procedures were in place to monitor all employees and contractors are receiving security awareness training. Additionally, we inspected a selection of current users to test compliance with the security awareness training procedures.
8. Inspected security awareness and training policies and procedures, and the training website and determined annual IT Security, Privacy Awareness, and Ethics training were required and specialized training was based on roles within HRConnect.
9. Inspected a list of application-specific training courses and determined application-specific training was offered for HRConnect.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

10. Inspected training records and determined training records were monitored and provided evidence that employees are receiving the appropriate training.

No exceptions were noted, other than the exception listed in test 5.

Access Control

Control Objective 3: Access to Facilities

Controls provide reasonable assurance that access to facilities is limited to appropriately authorized personnel.

Description of Controls

EBS Location

EBS' physical location has a security guard located within the lobby of the building requiring the signature of guest and escort by an EBS employee. The guest's signature is maintained in a hard copy log book at the guard station. Access to EBS' physical location is controlled using pre-numbered access cards to the elevators and floors. Access cards control access to facilities, as well as the physical access of computer equipment.

Physical access to facilities is gained after an employee/contractor completes the paperwork and fingerprints required for a background investigation. An access badge is issued to a new employee/contractor only after a favorable Special Agreement Check (SAC) is completed. The SAC is a limited investigation (or a series of checks) done only through special agreement between OPM and an agency. Access badges are required for entry and must always be displayed.

Each employee and contractor has an issued PIV card after the appropriate security approval. Employees and contractors must use their PIV cards to access their floors in the elevators and to enter the work area on the floor itself, as well. Signs on floor entrances instruct all personnel to use their badges and not allow others to "piggyback."

PIV Cards

Within the OCIO's Infrastructure and Operations is the Treasury Enterprise Identity Credential and Access Management (TEICAM). Its mission is to improve security, efficiency, and promote interoperability through Identity and Access Management for Treasury personnel, organizations, partners, and external agencies including EBS' HRConnect. The TEICAM provides requirements, coordination, management processes, technical coordination for personal identity verification, credential and access management compliance and solutions for HSPD-12. TEICAM and Federal Public Key Infrastructure (PKI) initiatives are established Treasury-wide. TEICAM capabilities

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

include: PIV Data Synchronization (PDS); Physical Access Controls (PACs); Logical Access Controls (LACs) for local, remote, and mobile devices, including Derived PIV credential infrastructure and issuance; Single Sign-On (SSO); Federation; Enterprise Identity Management; and PKI.

All users are required to go through the authentication process in order to access the system. Once logged in, users have access to pages and menus that are defined by their permission lists and roles. The data accessed is controlled by Row Level Security, based on each bureau's department tree.

Data Centers

Datacenter hard drives, storage devices, Storage Area Network (SAN) storage devices[1], removable devices, etc. must be pulverized and can never be traded-in to the vendor or disposed of as being surplus. The destruction of this equipment is tracked. Visitors accessing the Datacenter must be escorted while inside the Datacenter.

IRS Data Center Location

EBS performs site visit reviews to verify data center implementation of physical and environmental (PE) controls surrounding the HRConnect equipment annually across the EBS HRLOB systems. On behalf of Treasury EBS HRConnect, the data center sufficiently provides those inherited controls, such as physical access controls to the building and the individual data centers (no one is allowed in unless previously authorized or escorted by approved escort), physical access controls (armed building guards, identity checks, sign-in sheets, closed-circuit television (CCTV) cameras, locked doors, alarmed emergency exits), visitor access controls and escorting, fire protection and suppression mechanisms (smoke & ion detectors, sprinkler systems, fire extinguishers), protected and redundant power conditioning equipment and cabling, emergency power shutoff, temperature and humidity controls, water damage protection (raised floors, water detectors), information system backups, secure and redundant telecommunication services, and other controls. Based on the hosting center's policies, visitors accessing the Datacenter must be escorted while inside the IRS Datacenter and inside the Treasury Enterprise Infrastructure Operations Services (EIOS) facility module.

HRConnect resides within the IRS' Memphis (MEM) and Martinsburg (MTB) facilities; IRS Memphis serves as the primary site; hosting production services. IRS Martinsburg serves as the alternate facility. HRConnect inherits its Physical and Environmental controls from the IRS data center on which it resides and the Treasury EIOS hardware hosting services, which comply with Treasury and IRS security policies. EBS CyberSecurity validates IRS and EIOS controls (Physical and Environmental, and Access Controls, System Communication, Media Protection, etc.) via site

[1] A storage area network (SAN) is a secure high-speed data transfer network that makes a network of storage devices accessible to multiple servers.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

visits and checklists. HRConnect development and support staff inherit their physical access controls from the Treasury leased building staff that resides within and the Treasury network they access.

Tests of Operating Effectiveness and Results of Testing

1. Inspected EBS FY2018 annual site report of the IRS Datacenter and determined weaknesses were noted and communicated with Datacenter management.
2. Observed the security guard in the lobby of the building and determined they required signatures of guests and required guests to be escorted by EBS personnel.
3. Observed employees swipe their PIV card through the card reader to gain access to restricted floors and determined the floor entry was properly restricted.
4. Inspected PIV cards and determined access to floors within the building was controlled using PIV cards.

No exceptions noted.

Access to Computerized Applications and Sensitive Information

Control Objective 4: Access to Computerized Applications

Controls provide reasonable assurance that access to computerized applications and sensitive information is limited to appropriately authorized personnel.

Description of Controls

EBS HRConnect system stores PII data and the data is encrypted at rest and in transit. Access to HRConnect system is restricted to users with a valid logon identification and password or PIV card. Non-privileged users gain access to HRConnect through on-line account registration by entering a combination of their email address, the last four digits of their social security number, their last name, and a pin number that they create themselves upon registration. This process allows the user to then create a unique password that must be 12 characters long and must include at least one upper case and one lower case letter, one number and one special character. Users with access to PII are required to complete the HRConnect Program Office (HRCPO) Agreement to Safeguard Sensitive Data.

All passwords expire every 90 days and users are required to use the UserID or Password link to reset their password and facilitated via the Password Management System (PWMS). Users are also required to use the Forgot Password link after 3 failed login attempts. The Forgot Password link is located on the HRConnect login page. This process is the same as the account registration process

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

that requires the user to enter a combination of their email address, last four digits of their social security number, their last name, and a custom pin number.

Access to HRConnect is dependent on the level of access needed. Non-privileged level access is granted dynamically upon account registration. This includes Employee, Contingent Worker, and Manager basic level access. All managers get access to initiate actions. Managers can assign proxies to initiate, approve, or initiate and approve actions on their behalf. Access privileges are granted based on the level of access required to support the process (e.g. for HR - processor, specialist). Privileged user accounts in production are controlled by strong passwords. Passwords are locked after inactivity and are manually deleted by the EBS Helpdesk.

Privileged level access can be granted by Bureau Administrators at each customer agency via User Access Maintenance. More advanced privileged-level access and Super-level access can only be granted by the EBS Customer Solutions team and requires a Treasury Shared Service Center Security Access Form to be completed. Bureau/Sub-agency super and privileged users are created using forms requiring agency and supervisor approval. These forms are emailed to the Customer Solutions Team E-mail box. The Security Access form is required for the following access:

- Super User access, which grants users access to all panels and agencies in HRConnect.
- Privileged level access to HRConnect, which includes any roles not available to the agency via Bureau Maintenance User Access Maintenance. Examples of these roles include, but are not limited to, HR Super role and Servicing Bureau access.

The Treasury Shared Service Center Security Access form should be signed by the user, the user's manager, and the agency representative. The approved form is then emailed to Customer Solutions for setup. Customer Solutions will grant the access and notify the user of the UserID and password. Customer Solutions will then notify the agency that the access has been granted and the user has been provided with their credentials. User accounts are deactivated via the PAR process for terminating users. User IDs that have been deactivated due to termination is automatically locked. An automated process runs every night. First, it scans all the PARs for any users that are contingent workers or employees that are no longer active as of that day or prior. The process then updates those user profiles as follows: locks the account, removes the primary permission list, and removes all the roles. This prevents the account from accidentally being unlocked and being usable.

HRCPO Customer Solutions performs additional audits on user accounts. Privileged and Superuser accounts are analyzed by Customer Solutions quarterly to determine which accounts and roles are no longer needed due to termination or transfer. Health check reports are generated twice a month. The health check consists of several reports that are reviewed by Customer Solutions. Customer Solutions reviews the health check report to identify user accounts with duplicate IDs. Positions that are encumbered by more than one employee are forwarded to the

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

agencies for review. Active employees reporting to inactive positions are forwarded to the agencies for review. Separated employees that need to be removed from the PAR Approving Officials table and name changes to update the PAR Approving Officials table are reviewed by Customer Solutions. The health check review includes a review of the PAR Approving Officials table for both Terminated users and name changes.

The Treasury Shared Service Center Security Access form is also used to grant access to the following applications that are included in this audit review:

- Border Server
  - Customer Solutions collects the forms, ensures they are complete, and then forwards the form to the UNIX team for set up. The UNIX team communicates the userID and Password to the user. Once the account is set up, Customer Solutions notifies the agency that the account set up is complete.
- InCompass Privileged and Non-Privileged Access
  - EBS' Customer Solutions collects the forms, ensures they are complete, and then forwards the form to the InCompass team for setting up. Access is restricted to users with a valid logon identification and password. Once the account is set up, Customer Solutions notifies both the user (with the credentials) and the agency that the account set up is complete. Password reset requests are facilitated through automated email notification. Daily reports are provided to all users who have accessed the system within a specified number of days. Admin accounts are manually reconciled intermittently; non-admin accounts are inserted/reconciled by the HRConnect Data Feed.
- InTime
  - New users, transfers, and terminations are established through the HRConnect daily export file. Temporary passwords are sent via email to new users requesting them to change their passwords. Newly established passwords are valid for the specified number of days and then required to be changed. Invalid login attempts are limited upon which the user is locked out. Various audit functions are performed via the application menu of audits available. Treasury privileged user access is granted after completing access request form and obtaining supervisor approval. DOL privileged user access categories include several levels of access.

Complementary User Entity Controls

User entity auditors should determine whether user entities have established controls to provide reasonable assurance to properly grant access to the systems to users who have been vetted by their organization's security requirements. Additionally, reasonable assurance to properly provide appropriate levels of privileged user access to the systems to users who have a bona fide need and have met their organization's security requirements. Finally, user entity auditors must determine whether user entities have established controls to provide reasonable assurance to properly assign

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

security roles to users based on their role in the system (e.g. personnel specialists would hold the HR Specialist role vs. a manager who would hold the manager role in HRConnect).

Remote Access

An EBS supervisor sends an email to the Departmental Offices network authorizing employee/contractor's remote access. Once remote access is granted, the employee/contractor can use their workstation to remote access to the same systems they access at their duty station. Information provided in the authorizing email is used for completing a P4P form.

Tests of Operating Effectiveness and Results of Testing

1. Inspected the password control configuration and the management policies and procedures and determined the configuration agreed with management policies and procedures.
2. Observed an executed password reset and determined the reset process agreed with management policy and procedures.
3. Inspected a selection of HRConnect users' access privileges and job title and responsibilities and determined access privileges were appropriate for job title and responsibilities.
4. Inspected the SSP and determined access privileges of a Super User and Normal User were defined.
5. Inspected a selection of forms of HRConnect users' Bureau / Sub-agency Super User and determined they were completed.
6. Inspected the Super User quarterly review for the first and second quarters and inspected management policies and procedures and determined the Super User quarterly reviews agreed with management policies and procedures.
7. Inspected a selection of Health Check Reports and determined the reports were generated twice a month and reviewed by the Customer Solutions Section.
8. Inspected a selection of access request forms and employee supervisor emails and determined remote access to the Departmental Offices Remote Access (DORA) was granted after the employee's supervisor sent an email authorizing remote access.
9. Inspected a selection of P4P forms and authorizing emails and determined the information provided in the authorizing email was used for completing the P4P form.
10. Inspected a selection of users with PII access and determined the users completed records and signed HRCPO Agreement to Safeguard Sensitive Data. **Exception noted**. Eight HRCPO Agreement to Safeguard Sensitive Data forms out of ten selected for testing were not signed by the security officer. Additionally, the remaining two forms were signed by the security officer two months after the forms were signed by the employee and their supervisor.
11. Inspected the SSP and determined it required that data is encrypted at rest and in transit and whether PII breaches were required to reported to the proper organizations.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

12. Inspected the PeopleSoft password configuration and determined privileged user accounts in HRConnect Production Environment (HR PROD) were protected by strong authenticator management controls.
13. Inspected a selection of border server access users and determined users completed HRConnect User Access Request Form. **Exception noted**. One Treasury Shared Service Center Security Access form out of ten selected for testing was not signed by the user's manager. Additionally, one of the remaining nine forms was missing.

No exceptions were noted, other than the exception listed in tests 10 and 13.

Configuration Management Controls

Control Objective 5: Software Development and Maintenance Activities

Controls provide reasonable assurance that software development and maintenance activities are authorized, documented, tested, and approved as described in the HRConnect System Development Life Cycle (SDLC) methodology.

Description of Controls

EBS has documented the configuration management process for HRConnect applications that includes roles, responsibilities, reviews, and approvals of configuration changes.

The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the initiation of a project to develop a system to its disposition. The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system, is called the SDLC. EBS uses ClearQuest change management software to control changes for HRConnect and maintain application baselines throughout the SDLC. The ClearQuest change management software manages the approvals, audit trails, coding, testing, and publication of the software changes. The management software allows automated workflows and email notifications to ensure that appropriate team members are alerted in near real-time when action is required; and software changes, along with associated requirements, are documented. Production ClearQuest change requests are tested according to development organization guidelines and approved prior to implementation. Once approvals have been received, the change is migrated to the production environment by the change management software or an EBS staff member who is independent of application developers.

Proposed change requests (CRs) are submitted to the Intake team. These can be submitted by Customer representatives or internal team members. Proposed CRs are sent weekly to functional analysts and developers. Recommendations are then shared with the management team for

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

approval. If the CR is recommended to move forward, a Business Requirement Document (BRD) and Level of Effort (LOE) are created and shared with the customer.

CRs are discussed in the monthly Configuration Control Board (CCB) meeting and feedback is requested from the customers. EBS records the CCB minutes and distributes them to the participants. If the CR is recommended/selected, alternative impacts, both positive and negative, are documented if appropriate, and the Functional Design Document (FDD) is approved by the Director of HRConnect Products and the Functional Architect. If the CR LOE is less than 40 hours (data only update, one-time script, minor text changes to pages, emails, etc.), an FDD and/or Technical Design Document (TDD) may not be required. A waiver is submitted and documented for approval.

An EBS Developer performs a TDD review to walk through the changes and impact based on the FDD. The TDD is a working document and is completed at the end of development. The development and technical documentation are considered complete, when the CR includes:

- a functional design document or FDD waiver,
- a technical design document or TDD waiver, and;
- technical peer review performed as described in the Software Peer Review Procedure.

Minutes from the technical peer review session should be included in the technical data package for the CR on the shared J drive and ClearQuest.

Each stage/lifecycle is separate for purposes of creating an independent process (intake, design, development, testing, internal validation, and customer user acceptance). At the end of the cycle (whether internal or customer acceptance), approval is required for the changes made.

Tests of Operating Effectiveness and Results of Testing

1. Inspected the HRConnect SDLC and determined it was reviewed, approved, and updated.
2. Inspected a list of personnel authorized to access the information system for purposes of initiating changes, upgrades, and/or modifications to the system and determined EBS maintained the list.
3. Selected records identifying changes made to the information system and determined only authorized personnel initiated, tested, approved, and implemented changes to the system.
4. Inspected an FDD and determined the FDDs were used to document the functional design of the approved change request.
5. Inspected a selection of HRConnect change requests and determined change requests were reviewed and approved in review board meetings.
6. Inspected access lists and determined developers had access to the production environment.
7. Inquired with HRConnect management and inspected change control documentation, flowcharts, and forms and determined proposed CRs were submitted to the Intake team;

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

proposed CRs were reviewed weekly with functional analysts and developers, and recommendations were shared with the management team for approval.

8. Inspected a selection of BRD and LOE documents and determined BRDs and LOEs were created and if there was a recommendation to move forward with changes.
9. Inspected monthly board meeting minutes and determined CRs were discussed in the monthly CCB meeting and feedback was requested from the customers.
10. Inspected waivers and determined the waivers were submitted and documented for approval when an FDD and/or TDD was not required because the CR LOE was less than 40 hours.
11. Inspected supporting documentation and determined alternative impacts (positive or negative) were documented and the FDD was approved by the Director of HRConnect Products and the functional architect.
12. Inspected a selection of TDD and determined developers performed TDD reviews to walk through the changes and impact based on the FDD.
13. Inspected a selection of CR and determined CRs contained the appropriate development and technical documentation.
14. Inspected a selection of CR and determined approvals were performed for the changes made at the end of the stage/lifecycle.

No exceptions noted.

Control Objective 6: Processes and Procedures to Respond to Unusual Activity or Intrusion Attempts

Controls provide reasonable assurance that management has processes and procedures in place to monitor unusual activity and/or intrusion attempts.

Description of Controls

Manual security inspection is performed on all EBS Cisco firewalls. On behalf of a System owner and ISSO, EBS CyberSecurity security engineers conduct a monthly vulnerability assessment and system security configuration scans to identify network vulnerabilities. EBS analyzes the identified vulnerabilities and either mitigates the vulnerability or documents it is required for production processes. EBS scans the various layers of HRConnect based on Treasury policy and EBS CyberSecurity team formal SOP. Vulnerabilities are provided to System Owners and Technical staff for remediation. All monthly scans that are conducted by EBS cyber engineers are tracked in a Vulnerability Executive Summary spreadsheet. Findings are tracked for remediation, and vulnerabilities identified from monthly scans are added as POA&Ms based on policy's remediation schedule. EBS CyberSecurity manually inspects the security of the HRConnect firewalls and delivers reports semi-annually and upon changes.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

EBS' vulnerability management process follows Departmental policy on Patch Management and System Updates to ensure system flaws are identified, reported, and corrected. Patches are prioritized and approved through EBS and are tested on non-production systems prior to installation on all production systems.

Penetration testing is conducted annually to exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access to EBS' IT operational environment; specifically, to demonstrate whether technical weaknesses were present in EBS' computer systems that may allow employees or outsiders to inflict harm to, attack, and/or impact HRConnect.

Tests of Operating Effectiveness and Results of Testing

1. Inquired of EBS personnel with system and information integrity responsibitlites and inspected the HRConnect SSP and US Department of Treasury Network Vulnerability Assessment and determined EBS identified recently announced software flaws and potential vulnerabilities resulting from those flaws that may affect the information system.
2. Inspected EBS Technical Architecture Maintenance Records for two months and determined EBS installed newly released security patches, service packs, and hotfixes on the information system in a reasonable timeframe in accordance with EBS policy and procedures.
3. Inspected documentation of manual security inspections and determined the inspections were performed on the In-Time firewalls.
4. Inspected vulnerability scans and determined vulnerability scans were conducted monthly.
5. Inspected the results of penetration testing and determined penetration testing occurred annually.
6. Inspected the Vulnerability Executive Summary spreadsheets and determined the spreadsheets tracked all monthly scans that were conducted by EBS cyber engineers.
7. Inspected EBS documents and determined EBS employed malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses).

No exceptions noted.

Control Objective 7: Accuracy Testing Methods

Controls provide reasonable assurance that reconciliations, exception reports, and transmittal process are designed to ensure interfaces are working accurately.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Description of Controls

inCompass

After HRConnect data is transferred to CSOD, the inCompass program team performs an annual review process to evaluate the data feed to ensure that the information populating the system is still relevant and necessary for CSOD to work as designed. The inCompass program team looks at the current data feed and compares the data collected against the new functionality deployed or newly available data to determine potential efficiencies that could be gained through additional data elements or structurally changed data. If there are opportunities to make improvements, the inCompass program team works with the HRConnect team to institute these changes.

With an automated data feed, an error report is generated by CSOD each night, Monday through Friday, specifically identifying errors that prevent the system from updating core user information. The error report identifies the issue and allows for correction of the data from the source system before the next feed occurs. This data correction process is inherited from HRConnect. If there is an error, it is the responsibility of the participating agency's process owner to take appropriate steps to correct the findings. Follow-up communication with customers regarding interface variances is via email. The successful data interface is evidenced by customer email notification showing data feed log. User and organizational unit files are placed on the border server for customers to retrieve.

InTime

EBS' webTA is the name Kronos uses for their US Federal time and attendance solution. InTime is the name Treasury used to brand its specific implementation of webTA.

The HRConnect to webTA interface consists of four flat file interfaces. They are one directional in that data only flows from HRConnect to webTA. This data is used to establish and maintain user and accounting data in webTA in an automated fashion. All data transmitted to InTime is contained in fixed length, sequential 'flat' files. The data is transmitted Monday – Friday, and consists of the following four data sets:

- Organization Data (HRConnect's Customers' Data) – This file contains the organization tree. It only contains data when there is an organization update. When there is, HRConnect sends the entire organization tree to update webTA. Organization Structure data is extracted and transmitted only when needed for description or stats (active/inactive) changes to the departments contained in the structure. Structural changes (parent/child) that result in a new effective dated tree will require the entire Organization Structure to be transmitted for replacement within webTA.
- Employee Data – This file contains data elements for individual employees. When an employee is hired, rehired, separates, or has any data element change, HRConnect

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

generates a row of data for that employee and sends it to webTA. WebTA uses this data to automatically create, update, and deactivate user accounts. Employee Profile and Timesheet Profile data is extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of these file formats. Any error with a timesheet during the export will result in the timesheet being flagged as "action required" and the timesheet employee's supervisor is notified. All system administrators will also be alerted to any failed timesheets via the InTime notification system. A single timesheet failure will not prevent the rest of the timesheets from processing or being transmitted.

- Accounting Data – This file contains accounting strings for individual employees. HRConnect generates a row of data whenever there is a change to an account code and employee changes positions. WebTA requires this accounting data when transmitting timecards to the payroll provider. Common Government-wide Accounting Classification Structure (CGAC) data is extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of these file formats.
- Leave Data – This file contains different types of leave balances for individual employees. HRConnect generates a row of data with all leave balances for all employee on each file. WebTA uses these leave balances to update its own leave balances. Leave Balances data is extracted and transmitted bi-weekly from HRConnect Group 6-NFC.

Emails are generated from InTime and sent to the customer indicating successful transmission or exceptions. Logs of the interfaces are captured within InTime. The Interfaces are regularly scheduled for designated times throughout the week.

DOL Accounting

EBS accepts a daily delta file of accounting lines from the Department of Labor (DOL) financials application and applies changes and additions. Lines in the file must be coded as New, Replace, or Inactivate. New accounting lines are inserted into the HRConnect account code tables. Inactivated lines have a new row inserted into the HRConnect account code tables, making the row inactive. Replacement lines are inserted, the replaced lines are deactivated, and the replacement is noted in a secondary table to support programmatic updates to the account code assignments on individual positions. This is a one-way feed. Logs are written to the N drive nightly (Monday through Friday). Nothing goes back to DOL financials from the HRConnect application. These files are then provided to DOL. An automated nightly process is run to send new payroll related DOL accounting lines and changes to existing payroll related DOL accounting lines to HRConnect through border servers. EBS receives DOL's NFC files after payroll is run every Monday at 6 a.m.

Accounting lines that do not include all required fields will be reported as errors. This includes any accounting line that includes one or more Replaced fields but not the Replaced Effective Date. Interface data will be written to this table without manipulation beyond the addition of the date/time stamp. Records in error are reported on the Invalid Accounting Lines report. There is a

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

visual prompt for this on-demand report, letting the customer know when the report needs to be run.

With an automated data feed, an error report is generated by CSOD each night, Monday through Friday, specifically identifying errors that prevent the system from updating core user information. The error report identifies the issue and allows for correction of the data from the source system before the next feed occurs. This data correction process is inherited from HRConnect. If there is an error, it is the responsibility of the participating agency's process owner to take appropriate steps to correct the findings. Follow-up communication with customers regarding interface variances is via email. The successful data interface is evidenced by customer email notification showing data feed log. User and organizational unit files are placed on the border server for customers to retrieve.

Tests of Operating Effectiveness and Results of Testing

inCompass

1. Inspected data feed reports and determined they showed interface errors for customers.
2. Inspected emails and determined communication regarding interface variances took place.
3. Inspected email notifications showing data feed logs and determined there were successful data interfaces.
4. Inspected border servers and determined user and organizational unit files were available for customers to retrieve.

InTime

1. Observed an IT Specialist transmit files to InTime and determined all data transmitted to InTime was contained in fixed length, sequential 'flat' files.
2. Inspected a selection of daily Employee Profile and Timesheet Profile data from InTime and determined Employee Profile and Timesheet Profile data was extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of these file formats.
3. Inspected a selection of daily Accounting-CGAC data from InTime and determined Accounting-CGAC data was extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of these file formats.
4. Inspected a selection of Leave Balances data from InTime and determined Leave Balances data was extracted and transmitted on an ad-hoc basis from HRConnect and Group 6-NFC Leave Balance Interface TDD captured the process.
5. Inspected a selection of Organization Structure Data from InTime and determined the data was extracted and transmitted only when needed for description or status (active/inactive) changes to the departments contained in the structure.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

6. Inspected a selection of Organization Structure changes from HRConnect and determined the changes (parent/child) that result in a new effective dated tree required the entire Organization Structure to be transmitted for replacement within webTA.
7. Inspected a selection of timesheets and determined a process was in place to identify and follow up on timesheet errors.
8. Inspected the interface schedule and determined interfaces were regularly scheduled for designated times throughout the week.
9. Inspected the log of interfaces within InTime and determined a log of the interfaces was captured within InTime.
10. Inspected emails and determined emails were generated from InTime indicating successful transmission or exceptions.

DOL Accounting

1. Inspected the Accounting Interface Requirements Summary Document and determined an automated nightly process was run to send new payroll related DOL accounting lines and changes to existing payroll related DOL accounting lines to HRConnect through border servers.
2. Inspected records of EBS receipt of DOL's NFC files and determined EBS received DOL's NFC files after payroll was run every Monday at 6 A.M.
3. Inspected data feed error reports and determined a data feed error report regarding interface errors was generated Monday through Friday for all customers.
4. Inspected emails and determined that customer follow-up was conducted on interface variances.
5. Inspected a selection of customer email notifications and determined there were successful data interfaces.
6. Inspected access request forms and determined customers were properly authorized to retrieve files from the border server.

No exceptions noted.

Control Objective 8: Customer Interagency Agreements

Controls provide reasonable assurance that Customer Interagency Agreements are appropriately monitored in accordance with established procedures to ensure efficiency and performance results.

Description of Controls

EBS establishes an Interagency Agreement (IAA) with the Requesting Agency requesting services performed by EBS' Shared Services Programs (SSP) and the Department of Treasury. The IAA conforms to the government-wide guidance prescribed by the Bureau of the Fiscal Service (Fiscal

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Service) in TFM, Vol. I, Part 2, Ch. 4700, App. IO, (June 2011). The IAA authorizes SSP to provide the Requesting Agency service as described in the service description(s).

EBS works closely with its customers. Each year, EBS and its customers agree to the scope and nature of services to be provided by EBS, as well as responsibilities of the customer, as documented within the IAA.

EBS' customers participate in survey polls conducted by the General Services Administration (GSA) as well as surveys conducted by Treasury. EBS reviews the annual customer service survey provided by GSA to the ranking of EBS service. The results of the Treasury HRConnect surveys are discussed during the monthly configuration control board meetings. EBS documents changes to IAA using form 7600 A&B, as well as product-specific addendums. EBS does not have control of the questions or the timeliness of the surveys.

Tests of Operating Effectiveness and Results of Testing

1. Inspected email support and determined customer service surveys were performed by the Treasury.
2. Inspected customer surveys and determined annual surveys for each customer were performed.
3. Inspected meeting materials and determined the results of polls and surveys were discussed during the monthly configuration control board meetings.
4. Inspected IAA forms and determined changes to agreements were documented using IAA forms, as well as product-specific addendums.

No exceptions noted.

Control Objective 9: Secure Interface Processes

Controls provide reasonable assurance that processes are in place to establish secure interfaces.

Description of Controls

Border Servers

The HRConnect border server securely exchanges interface files between HRConnect and user entities. The border server provides special security measures to ensure that all files are scanned for malware and are only accessible by approved individuals.

User entities place their interface files in a specified directory in the user entity server. The user entity accesses the HRConnect border server to pull or push interface files.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

For user entities who contracted with a third-party hosting vendor to transfer interface files, HRConnect uses an automated process to push or pull interface files with the hosting vendor. The third-party hosting vendor does not have access privileges to HRConnect border server.

Interface files are encrypted in transit. Only the Secure File Transfer Protocol (SFTP) and Connect: Direct FTP+ protocols are allowed for file transfers.

Secured Interface

New interface requests are handled through the EBS HRConnect change control process. EBS CyberSecurity Team/ISSO reviews the change request that includes the information of data to be transmitted to or from HRConnect. The CyberSecurity Team inspects the information to determine whether the data is appropriate and can be adequately secured. The CyberSecurity Team and EBS Technical Architecture (TA) meets with the user entity and third-party vendor, if any, to discuss and identify specific security issues. Once the security issues are resolved, the EBS CyberSecurity Team approves the user entity request to begin testing of the connectivity and transfer of data. When the new interface is approved, the EBS CyberSecurity team creates an ISA if required. An updated ISA is required every three years.

The user entity provides technical contacts to the TA team and to the third-party vendor, if necessary. The user entity or third-party vendor provides IP addresses of user entity's data required to transmit the data to the EBS border servers (both test and production EBS border servers). The EBS Deployment team provides the User Entity's technical contact with an EBS Access Request Form.

The EBS TA team creates a Fiscal Services Change Request (CR) requesting the Fiscal Services update firewall rules to allow the transmission between the user entity or third-party vendor to the EBS border servers. The CR may take two to three weeks for processing from initiation to approval, to scheduling, and to completion.

The EBS TA team prepares a maintenance plan to update firewall rules to permit transmission between the user entity's third-party vendor order servers and EBS border servers.

Data exchanges with third-party vendors are encrypted at rest using the recipient's PGP public key. For example, data sent from the border server to the vendor is encrypted at rest using the vendor's public PGP key. For data retrieved from the vendor and placed on the border server, the data is encrypted at rest using the HRCPO public PGP key.

The EBS TA team establishes password-based connectivity to the third-party vendor servers using SFTP and the newly provided credentials. Then the EBS TA team provides the Treasury SSH public key to the partner and requests that they add the Treasury public key to the partner's PKI KeyStore. Once this is completed, the EBS TA team can establish key-based authentication

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

instead of password-based authentication. Once key-based authentication is established, the EBS TA team automates the file transfer process. The EBS Deployment team provides the connectivity information (Unix ID and password, EBS border server name/IP address, and UNIX directory where interface files are stored) to the User Entity's technical contact.

The EBS TA team and third-party vendor test the basic file transfers and PGP encryption/ decryption capabilities.

The EBS developer responsible for the interface program creates a ClearQuest Technical Architecture (CQ TA) Work Order to have Control-M automate the pushing and pulling of files between the Control-M server and the EBS border server. The TA Work Order contains information including the names of the files being transferred, the size of the files being transferred, and the transfer schedule. The EBS developer refers to the CQ TA Work Order in the interface program Customer Service Request (CSR) migration notes so that the Control-M updates are made at the same time as the interface program is migrated.

The EBS Security team approves the production implementation, and file transfer automation is enabled in production.

Complementary User Entity Controls

User entity auditors should determine whether user entities have established controls to provide reasonable assurance that the User Entity's technical contact tests connectivity from the User Entity's border server to the EBS border server using SSH and SFTP. It is recommended, but not required that the User Entity's technical contact places the User Entity's border server public key on the EBS border server so that certificate-based authentication can take place. The User Entity's technical contact should also test file transfers (pushes and pulls) between the User Entity's border server and the EBS border server.

Tests of Operating Effectiveness and Results of Testing

1. Inspected a selection of new interface documentation and determined the Deployment Team reviewed the documentation to determine whether it was approved by the Security Team.
2. Inspected a selection of EBS Access Request Forms and determined the Deployment Team provided the User Entity's technical contact with an EBS Access Request Form.
3. Inspected a selection of technical contacts and determined the EBS TA team provided the connectivity information to the User Entity's technical contact.
4. Inspected supporting documentation for a selection of CQ TA Work Orders and determined the EBS developer responsible for the interface program created a CQ TA Work Order to request Control-M to automate the pushing and pulling of files between the Control-M server and the EBS border server.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

5. Inspected a CQ TA Work Order and determined the EBS developer referred to the CQ TA Work Order in the interface program CSR migration notes so that the Control-M updates were made at the same time as the interface program was migrated.

No exceptions noted.

Control Objective 10: Subservice Organizations

Controls provide reasonable assurance that EBS monitors subservice organizations and tests for compliances with complementary user entity controls.

Description of Controls

Memphis Data Center

EBS reviews control at the MDC annually and issues a site report. The IRS Memphis TN data center facility provides a secure data center to Treasury Enterprise Infrastructure Operations Services (EIOS) within turn provides infrastructure for HRConnect productions data.

EBS reviews control at the MDC annually and issues a site report. The IRS Memphis TN data center facility provides a secure data center to Treasury EIOS within turn provides infrastructure for HRConnect productions data.

National Finance Center

Subservice Complementary User Entity Controls

EBS reviews SSAE 18 results or other control-related documentation provided by subservice organizations to determine whether deficiencies (if any) affect subservice organization controls that in turn may impact the financial related reporting of HRConnect systems. The EBS CyberSecurity team reviews interconnected subservice organizations' systems' application Security Assessment and Authorization (SA&A)documentation: the EBS CyberSecurity team performed a SA&A Documentation Review Visit of the NFC Payroll/Personnel System (PPS) application in 2018; to review an interconnected system's FISMA status.

Complementary User Entity Controls

User entity auditors should determine whether user entities have established controls to provide reasonable assurance that SINQ errors, HCUP Status, and mismatch cases are corrected to ensure transactions are processed. The user entity auditor should also determine whether user entities have

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

established controls to provide reasonable assurance that the mismatch tables are reviewed and corrected.

Tests of Operating Effectiveness and Results of Testing

1. Inspected MDC site report dated 6/16/18 and determined EBS tested physical and environmental controls and issued recommendations.
2. Inspected the Report on National Finance Center's Description of Its Payroll/Personnel and Application-hosting Systems and the Suitability of the Design and Operating Effectiveness of Its Controls For the Period October 1, 2016 through July 31, 2017 and determined Subservice Complementary User Entity Controls were listed.
3. Inspected EBS monthly User Log-in reports and determined EBS reviewed reports and emails were sent to users with an inactive date of 30 days, 60 days, or 120 days. Additionally, and determined EBS made determinations concerning the need for user accounts based on inactivity.
4. Inspected a selection of daily reports and determined the number of actions sent and received on the NFC Inbound/Outbound data feed was the same.
5. Inspected database table-driven edits and determined they prevented users from entering invalid conditions online, and they ensured that data processed was complete, accurate, and valid before transmitting to NFC (master data source).
6. Inspected database table-driven edits and determined EHRI edits, Common edits (priority SINQS and agency unique), agency-specific edits, and Field Tuning edits were performed.
7. Inspected the Match and Lock Action processes and determined the Match process was completed daily on the inbound file received from NFC via a Control M job run (match job) and took data from the NFC Daily inbound file and HRConnect data, loaded the data to tables, compared the data finding row matches/mismatches, then compared at a data level.
8. Inspected DI-All Match Status and determined EBS tracks the status.

No exceptions noted.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

V. OTHER INFORMATION PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Background

The information included in Section V, "Other Information Provided by Enterprise Business Solutions" is presented by management of EBS to provide additional information and is not a part of EBS' description of its HRConnect system, made available to user entities during the period September 1, 2017 to July 31, 2018. Information about EBS' continuity planning and management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description of the HRConnect system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the HRConnect system.

Contingency Planning

Back-up – Cornerstone OnDemand

CSOD, a SaaS application, is responsible for data backup and recovery. Data is a primary concern for Cornerstone and its User Entity , including the backup of critical and confidential data. Cornerstone performs daily backups of the full database and hourly transactional backups to separate hot disks. Two days of hot backups are stored on a local SAN disk for immediate recovery. Cornerstone performs full backups and daily differential backups of our data onto tape. Daily backups are stored for one-week, weekly backups for five weeks, and monthly backups for six months. All backups are encrypted before they are written to tape and reside in an encrypted mode on the tapes (AES-256). Iron Mountain collects tapes each week and transports them in locked boxes to a secure vault. Cornerstone uses Iron Mountain locations in Compton, California facility, and Cowley in Oxford, UK

System Backup – HRConnect

A contingency plan has been developed and is reviewed and/or updated annually. The most recent annual review of the Contingency Plan occurred on May 17, 2018.

EBS reviews and updates the HRConnect Contingency Plan (Disaster Recovery Plan) annually; as indicated by updated plans in 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016,2017 and 2018. The CP/DR Plans are updated by the EBS Technical Architecture group after annual CP/DR testing is performed. The plans are corrected for discovered discrepancies and to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

The Contingency Plan includes directions/checklists for coordination with other organization elements (e.g., for HRConnect, the COOP plan to recover the system in IRS Memphis, TN data center facility via the IRS Martinsburg, WV data center).

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

The Recovery Time Objective (RTO) is seventy-two (72) hours and Recovery Point Objective (RPO) is one (1) hour. If the plan is to be activated, the Disaster Recovery Coordinator notifies the Information System Security Manager (ISSM), the Customer Solutions Team Leader, and the Technical Architecture Team and informs them of the details. One-to-one mirroring is also available.

At the end of the Recovery phase, the HRConnect application is available, as well as the border server and Control-M batch processing. However, the other environments hosted in MEM are not available in MTB. These environments include the HRRPT reporting system, the DCPOM Operations support environment, training, development, and testing. Border server services include access by third-party services to allow data access via certificate-based authentication. HRConnect has developed a Business Impact Analysis (BIA) as of January 26, 2015 Version 1.0 and the "HRConnect Disaster Recovery Plan – May 17, 2018" to support the RTO identified in the Contingency Plan. DataGuard, Oracle Log switch, and NetBackup enable the HRConnect Team to meet the RTO. The BIA assists the Contingency Planning Coordinator to streamline and focus their contingency plan development activities to achieve a more effective plan. The BIA also complies with the Department of the Treasury's IT security policy for contingency planning as specified in TDP 85-01. The BIA complies with the following supplemental security policies issued by the Department of the Treasury Chief Information Officer:

a) Testing of Contingency Plans, TCIO-M-06-04, June 2006; and
b) Supplemental Information on Contingency Planning, TCIO M 07-02, February 2007.

The Contingency Plan Test checklists include coordination with other critical organization elements (e.g., for HRConnect the COOP Plan to recover the system to IRS Memphis, TN data center facility, IRS Martinsburg, WV, Customer Solutions (customers' notification), Treasury BFS TIC, Cisco, EMC SAN, IRS Telecom, Bureau of Fiscal Services (Fiscal Service) for testing, Business Intelligence systems (WARS), R&D, etc.).

EBS tests the contingency plan with the alternate processing site. The IRS MTB in Martinsburg, WV is used as the alternate operating facility in the event of a catastrophic disaster at the production data center in Memphis. The alternate site equipment is rebuilt, and production is tested at the alternate site during the live tests. Other critical business partners, such as Cisco, are also included in the tests.

Personnel are periodically sent to the CP/DR site to check equipment and familiarize themselves with the HRConnect installation and equipment. The alternate DR site has a full database recovery of the IRS Memphis, TN data center facility. Daily, all data is written to the alternate data center facility and on the DataGuard standby database.

The Memphis and Martinsburg Data Centers Teams are responsible for providing key services at the Memphis and Martinsburg Data Centers, including enterprise network infrastructure, SAN and the data backup services in support of the HRConnect production environment at Memphis and

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Martinsburg. The SAN is not part of the HRConnect accreditation boundary per Technical Architecture team.

The alternate storage site for the HRConnect in IRS Memphis, TN facility is the IRS Martinsburg, WV data center facility. The IRS Martinsburg, WV data center facility is geographically separated from the Memphis data center facility by over 830 miles.

System and configuration files are copied via protected VPN from the IRS Memphis system to the IRS Martinsburg data center facility on a daily and near real-time basis. The Oracle DataGuard product replicates the transaction logs across the network in real time and those transactions are applied to a standby database in IRS Martinsburg, WV data center facility. The HRConnect area at IRS Martinsburg, WV data center facility is under lease exclusively to Treasury Information Operations (IO) and operated by Treasury IO as the HRConnect DR site.

System backups are transmitted daily to this site and the Oracle database replicates the minute-to-minute transactions to this site, as well. The IRS Memphis, TN data center facility contains a complete current backup of systems and data. Backups include all servers in IRS Memphis, TN. Full and partial backups staggered with files going to NetBackup and hence to IRS Martinsburg, WV data center facility for offsite storage. Backup logs are managed by the Windows SA.

In order to achieve the RTO of 72 hours and the 1-hour RPO, HRConnect uses the Oracle DataGuard, which enables transaction logging on every Oracle log. The Oracle DataGuard product replicates the transaction logs across the network in real time, and those transactions are applied to a standby database at the IRS MTB in Martinsburg, WV. All transaction logs are sent from MEM (primary site) to MTB (alternate DR site facility) every 20 minutes using Oracle Log Switch to keep data close to real-time. In addition, to enable data replication to the MTB, NetBackup and Networker are utilized with Solaris RSYNC technologies.

HRConnect utilizes the Disk to Disk lifecycle methodology via the DataDomain appliance to retain data for one year or less. The data is then replicated to another DataDomain appliance in our disaster recovery facility in the IRS Martinsburg, WV data center facility and kept for 90 days. Data that is retained longer is then sent to the DD990 and is de-duplicated and compressed. The "Networker and NetBackup Checklist" is available in J:\Infrastructure\Disaster Recovery\2016 HRC MEM-to-MTB\Checklists and is used to monitor the backup processes.

All the systems at the primary site are backed up to files on a daily basis. The backup files are replicated to the alternate data center facility every 20 minutes. The DR facility serves as the separate offsite storage location. Files can be recovered from either the on-site SAN or remotely from the IRS Martinsburg, WV data center facility when a primary system (IRS Memphis, TN) must be recovered.

EBS Backup/Restore System is comprised of several components: EMC NetWorker Enterprise Backups, Veritas NetBackup, and DataDomain appliances. The system executes and manages a

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

series of scripts to back up data files, and archive logs, audit files, and operating system files. The Oracle DataGuard product replicates the transaction logs across the network in real time, and those transactions are applied to a standby database at the IRS MTB in Martinsburg, WV. The data is then replicated to another DataDomain appliance in the disaster recovery facility in the IRS Martinsburg data center facility and kept for 90 days.

EBS utilizes the Oracle 11gR2 DataGuard tool for data backup. DataGuard aids in establishing and maintaining secondary "standby databases" as alternative/supplementary repositories to production "primary databases." DataGuard provides high availability for a database system. It can also reduce the human intervention required to switch between databases at disaster-recovery ("failover") or upgrade/maintenance ("switchover") time. DataGuard uses Oracle net to transfer files from the primary server to the standby server.

There are three backup policy groups in effect for IRS Martinsburg servers:

1. File Systems – The basic operating system (OS) and application file systems on every UNIX server are fully backed up once a week, with incremental backups taken daily. The backups are retained in the IRS Memphis for one year (currently) and at Martinsburg for 90 days before being overwritten on backup disk. This would be the data set used to completely restore a server in the event of a failure or to recover an individual OS or application file.
2. Database Backup – All Database backup file systems (/ORABACKUP and /QFSREFRESH, plus the export scripts in /ORACLE/HOME/EXPORT) receive an incremental backup taken daily. The data from this backup policy is retained in the IRS Memphis for one year (currently) and 90 days at Martinsburg before being overwritten. The policies for this group are the HRPROD and NonProd_DB_Backups.
3. Disaster – NetBackup backups a replication from Memphis to Martinsburg and vice versa.

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig