Audit Report

OIG-18-011

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, 2016, to August 31, 2017

November 9, 2017

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

November 9, 2017

MEMORANDUM FOR DEBRA D. VESS
ASSOCIATE CHIEF INFORMATION OFFICER – 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, 2016, to August 31, 2017

I am pleased to transmit the attached subject report. Under a contract monitored by our office, RMA Associates, LLC (RMA), an independent certified 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, 2016, to August 31, 2017;

- 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, 2016, to August 31, 2017, and subservice organizations and user entities applied the complementary controls assumed in the design of EBS' controls throughout the period September 1, 2016, to August 31, 2017; and

- except for the finding described below, that is required to be reported in accordance with *Government Auditing Standards*, the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2016, to August 31, 2017, if complementary subservice organization and user entity controls, assumed in the design of EBS' controls, operated effectively throughout the period September 1, 2016, to August 31, 2017.

EBS states in its description for its Control Objective 13, that "Controls provide reasonable assurance that EBS monitors subservice organizations and tests for compliance with complementary user entity controls." However, as noted in Section IV of this report, EBS did not provide sufficient documentation to indicate that EBS monitored or tested complementary user entity controls of its subservice organizations during the period September 1, 2016, to August 31, 2017. As a result, controls were not operating effectively to achieve the Control Objective 13.

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 31, 2017, 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 Services and on the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period
September 1, 2016 To August 31, 2017

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 Services and On the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period
September 1, 2016 To August 31, 2017

Table of Contents

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, 2016, to August 31, 2017, (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, 2016, to August 31, 2017. 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: Memphis Data Center (MDC) and National Finance Center (NFC) for hosting services. 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 has 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 that 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, 2016, to August 31, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our modified 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.

Basis for Qualified Opinion

EBS states in its description for its Control Objective 13, that "Controls provide reasonable assurance that EBS monitors subservice organizations and tests for compliances with complementary user entity controls." However, as noted in Section IV of this report, EBS did not provide sufficient documentation to indicate that EBS monitored or tested complementary user entity controls of its subservice organizations during the period September 1, 2016, to August 31, 2017. As a result, controls were not operating effectively to achieve the Control Objective 13.

Opinion

In our opinion, except for the matter referred to in the preceding paragraph, 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, 2016, to August 31, 2017.
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, 2016, to August 31, 2017, and the subservice organizations and user entities applied the complementary user entity controls assumed in the design of EBS's controls throughout the period September 1, 2016, to August 31, 2017.

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

3. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period September 1, 2016, to August 31, 2017, if complementary subservice organizations and user entity controls assumed in the design of EBS' controls operated effectively throughout the period September 1, 2016, to August 31, 2017.

In accordance with *Government Auditing Standards*, we are required to report all deficiencies that are considered to be significant deficiencies or material weaknesses in internal control; fraud and noncompliance with provisions of laws or regulations that have a material effect on the fairness of the presentation of management's description of the HRConnect system, the suitability of the design of EBS' controls relevant to user entities' internal control over financial reporting, and the operating effectiveness of those controls (the subject matter); and any other instances that warrant the attention of those charged with governance. We are also required to obtain and report the views of responsible officials concerning the findings, conclusions, and recommendations, as well as any planned corrective actions. We performed our examination to express an opinion on whether the subject matter is presented in accordance with the criteria described above and not for the purpose of expressing an opinion on the internal control over the subject matter or on compliance and other matters; accordingly, we express no such opinions. Our examination disclosed a finding that is required to be reported under *Government Auditing Standards* and that finding, along with the views of responsible officials, are described in the attached Finding Schedule.

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, 2016, to August 31, 2017, 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, LLC

RMA Associates

Arlington, VA
October 31, 2017

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

Enterprise Business Solutions
Finding Schedule
For the Period September 1, 2016, to August 31, 2017

Criteria: Control Objective 13: Subservice Organizations - Controls provide reasonable assurance that EBS monitors subservice organization and tests for compliances with complementary user entity controls.

Condition: The subservice organization designed its service with the assumption that certain controls would be implemented by EBS in order to achieve certain controls objectives that cannot be achieved by the subservice organization alone.

Sufficient documentation was not provided to indicate that EBS monitored its subservice organizations' Statement on Standards for Attestation Engagements (SSAE) No. 18 report or other control related documentation provided by subservice organizations. As a result, controls were not operating effectively to achieve the Control Objective 13: Controls provide reasonable assurance that EBS monitors subservice organizations and test for compliances with complementary user entity controls.

Cause: EBS did not maintain evidence of monitoring and testing of subservice complementary user entity controls.

Effect or Potential Effect: Without accurate records of monitoring and testing of subservice complementary user entity controls, EBS cannot demonstrate through its documentation whether it properly performed the complementary user entity controls and accordingly cannot demonstrate through its documentation whether the subservice controls operated as intended.

Management's Response: Treasury is reviewing the HRConnect Control Objective 13: Monitor and Control Subservice Organizations process to ensure it meets the control going forward.

II. MANAGEMENT ASSERTIONS PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

October 31, 2017

We have prepared the description of Enterprise Business Solutions' HRConnect Services 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 ,2016, to August 31, 2017, (description) for user entities of the system during some or all of the period September 1 ,2016, to August 31, 2017, 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, 2016, to August 31, 2017, 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.

(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.

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 Services 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, 2016, to August 31, 2017, 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, 2016 to August 31, 2017. 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 that manual controls were applied by individuals, who have the appropriate competence and authority.

We also state in our description that that controls are in place to provide reasonable assurance that EBS monitors its subservice organizations and tests for compliances with complementary user entity controls. However, since sufficient documentation was not provided, this control was not operating effectively throughout the period September 1, 2016, to August 31, 2017. This resulted in the non-achievement of the control objective 13: Controls provide reasonable assurance that EBS monitors subservice organizations and test for compliances with complementary user entity controls.

Except for the matter described in the preceding paragraphs, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period September 1 ,2016, to August 31, 2017 achieve those control objectives.

/s/

Nicolaos Totten
Associate Chief Information Officer (Acting)
Enterprise Business Solutions
Office of the Chief Information Officer
U.S. Department of the Treasury

Date: October 31, 2017

III. DESCRIPTION OF CONTROLS PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

OVERVIEW OF OPERATIONS

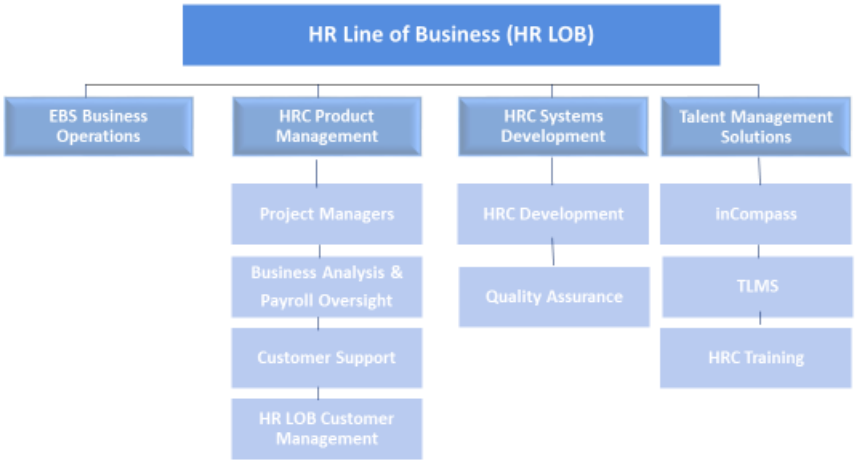
This examination only covers the products and services provided by EBS relating to the HRConnect system. In 2005, the Office of Personnel Management awarded EBS the Human Resources Line of Business (HRLOB) status, a certification which identifies its software products and services as a "best practice" within the federal sector. As an HRLOB Shared Services Provider, the HRConnect Services 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 Services is Treasury's enterprise human resources system. HRConnect Services is based on a combination of (a) web -based solution built on PeopleSoft commercial-off-the-shelf (COTS) software, (b) Software as a Service (SaaS) platforms. (e.g. Talent Management). HRConnect Services transforms core back-office 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 Services supports the common HR Line of Business 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, FAIR Act, 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 Services facilitates increased efficiency and overall productivity for its customers. The mission of HRConnect Services 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.

Figure 1, HRConnect Products and Services Chart, appears below

(Figure 1) HRConnect Products and Services



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

Control Environment

HRConnect, the Treasury Shared Service Center (TSSC) HR Line of Business, resides within the office of the Associate Chief Information Officer for Enterprise Business Solutions and is under the direction of the Office of the Chief Information Officer for the Department of Treasury. 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 address 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 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

HRConnect management and supervisory personnel monitor the quality of internal control 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 Actions and Milestones (POA&M) as a tool to document the planned remedial 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 EBS'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 delineate s resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. Quarterly, EBS reviews POA&M items and plans of action and milestones for consistency with EBS risk management strategy and organization-wide priorities for risk response actions.

Information and Communication

HRConnect system security plan 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 system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. The plan includes security-related documents for the information system such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, and security configuration requirements.

EBS controls the HRConnect System Security Plan by placing the plan in the Treasury FISMA Inventory System (TFIMS). TFIMS provides functionality to collect and manage data required by the Federal Information Security Management Act of 2014 (FISMA). TFIMS features include:

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

Self-Service

HRConnect has self-service components that 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, and HR Professionals. HRConnect features/functionality includes:

- Personnel Action Requests (PAR): PARs may be initiated online by Managers, their Proxies, and Detail Managers, and;
- HR specialists: HR staff can process a full suite of OPM-approved transactions (over 132 PAR actions) in HR Connect.

Change Requests

Customers proposed change requests (CRs) are submitted to the Intake team. Functional analysts and developers review the CRs weekly and share with the management team for approval. If approved a Business Requirement Document is prepared and Level of Effort is created and shared with the customer. CRs are discussed in the monthly configuration control board meeting and feedback is requested from the customers.

Change Control Board

EBS has established and a Change Control Board (CCB) that plays the role of gatekeeper in deciding which changes may be acted upon and introduced into HRConnect. The CCB deliberately considers the potential effect of a proposed change on the functionality and secure state of the system. The CCB reviews each proposed and implemented modification. The Board accepts or provides feedback on why they would not accept each proposed change.

Change Management Software

EBS use ClearQuest for change management software. ClearQuest manages workflows to control and enforce software and configuration development processes from requirements definition through production from requirements definition through the production environment. For Database changes ClearQuest issue A ClearQuest Technical Architecture (CQ TA).

HR Connect System Management Team

The HRC Product Management team is responsible for the management, operations, maintenance, and enhancement of the HRConnect. The team provides project management during new customer implementations. The team interacts with various levels of the customer organization to gather, document, review and approve all functional requirements for enhancements to the systems and interfaces. The team analyzes, defines, and documents human resources functional requirements and writes functional design documents; and coordinates the customer User Acceptance Testing (UAT) process. HRConnect's UAT is a structured testing process that makes sure that all user requirements are performing as the user wants and expects.UAT is the last phase of the software testing process. During UAT, HRConnect's customers test the software to make sure it can handle required tasks in real-world scenarios, according to specifications.

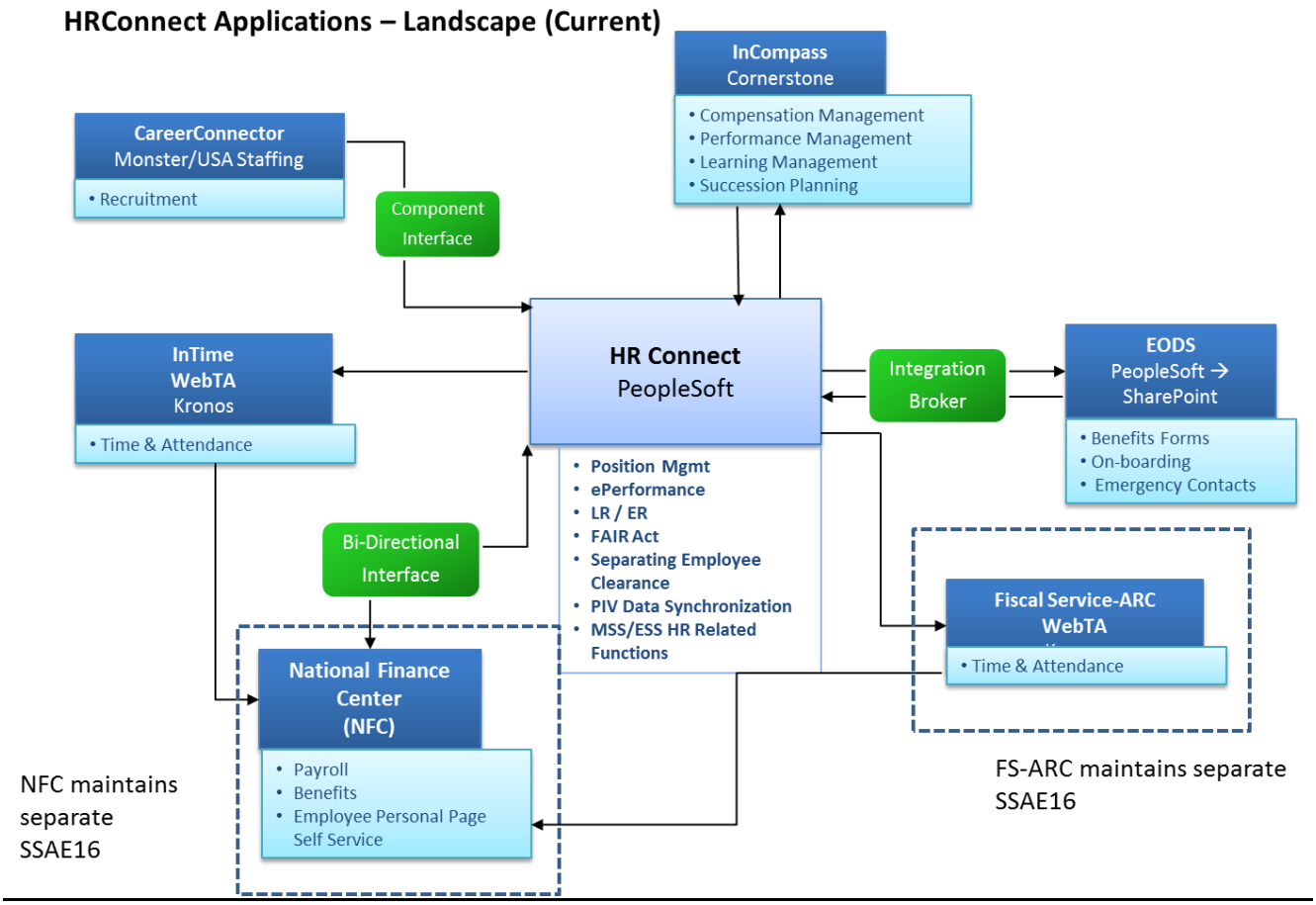
Interconnection Service Agreement (ISA) and the Interagency Agreement (IAA)

Enterprise Business Solutions establishes the HRConnect ISA and IAA with our customers. The intent of the ISA is to establish an agreement between the Department of Treasury OCIO EBS and the customer for the express purpose of exchanging personnel data between the HRConnect and our customers. The Security Agreement supports the security requirements of passing information directly between HRConnect and its customers. The ISA is updated and re-signed every three years and reviewed annually by the Treasury Information System Security Officer (ISSO), and verified by DO CISCO Information System Security Manager (ISSM).

The IAA forms 7600 A&B are established between federal agencies describing the general terms and conditions of the agreement. The IAA is reviewed annually by EBS and the agency if agreement period exceeds one year.

Systems and Interfaces

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



Note: HRConnect does not automatically feed WebTA this is done manually.

HRConnect

HRConnect Core supports the common HR Line of Business 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, SSN, Salary, etc.
- Employee skills, education and certificates
- Managers can manage Personal Action Processing and awards
- Workflow capability enables HR and Budget office to control position management
- FAIR Act

- Separation Employee Clearance

HR Specialists can approve and initiate position related actions, manage payroll documents and benefits There is a payroll interface which transmits the payroll data to the National Finance Center. 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 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 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 - collect logs from multiple types of IT systems for correlation and monitoring system activities with alerts. Splunk is also used for log retention.
- TripWire - is used to monitor files on systems for file integrity.

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 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 Human Resource systems.

The inCompass program sits on the Software-as-a-Service (SaaS) application Cornerstone OnDemand (CSOD). EBS has worked with CSOD to design inCompass to meet unique Federal needs such as FedRamp security requirements, and Office of Personnel Management (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.

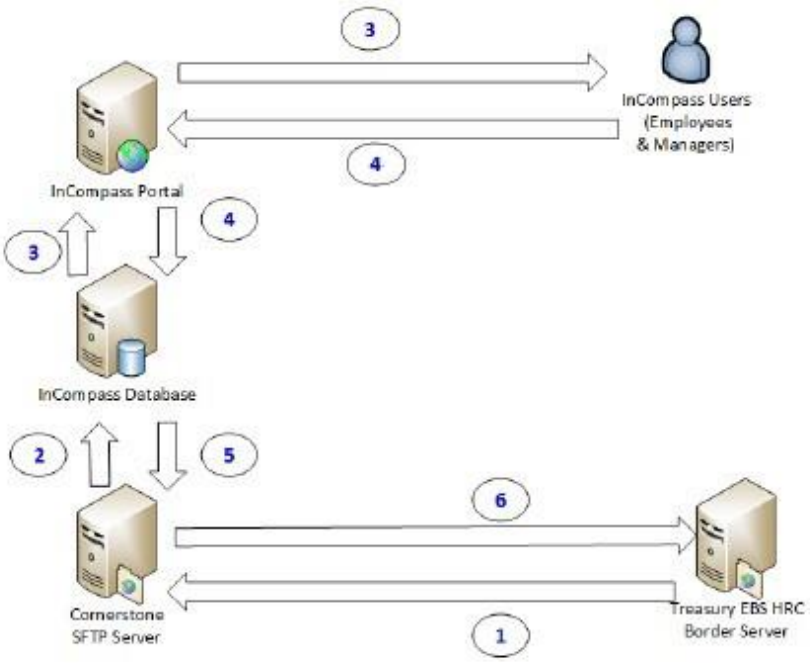
No Social Security numbers or birthdates are ever stored or processed within the inCompass environment.

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. inCompass application calls data from the database for presentation to the user, based on the module the user is accessing.
3. inCompass user enters provides information to complete forms that are passed by the application to the respective database.
4. Data extracted from inCompass databases to the inCompass SFTP server.
5. HRConnect Border Server pulls data from the inCompass SFTP via 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 Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules. Additional information about the contents of the data feeds is located in the ISA between Treasury and inCompass. End users and administrators access their inCompass portals via web browsers on TCP port 443. All configuration and other portal administration functions are performed through the user's web browser over port 443. 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.

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



InTime

Enterprise Business Solutions hosts WebTA 4.2 from Kronos as its time and attendance solution for the Department of Labor. 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 Linux platforms with an Oracle database backend. Currently, there are two web/app servers with the ability to scale to as many more as are 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.

Treasury maintains a continuity of operations plan for InTime. To support the plan, InTime uses database replication between its primary site in Reston, Virginia and its alternate site in Denver, Colorado. This process ensures that the disaster site is never more than one hour behind production and can be brought online within eight hours after a declared disaster in the primary site. The continuity of operations plan is tested once per year in accordance with FISMA policy.

For Cornerstone OnDemand, business continuity planning is viewed as a holistic approach for the entire business. As such, the activities involve business management from all functional, business, and product areas, including administrative, human resources, IT support functions, and key product lines. The Business Continuity Plan (BCP) Team is responsible for overseeing the development of the Program. They approve the written plans and ensure that senior management invests sufficient resources into planning, monitoring, and maintaining the BCP.

Cornerstone's Disaster Recovery/Business Continuity Plan defines plans, procedures, and guidelines for the Company in the event of disaster. Specifically, the plan establishes procedures for recovering business operations, internal data, systems, and critical internal functions to maintain Cornerstone as an on-going concern in the face of unexpected events.

The plan has the following primary objectives:

- Identify critical systems, services, and staff necessary to maintain and/or restore Cornerstone business operations and internal functions.
- Provide guidelines for the communication of activities and status to both Cornerstone staff and client personnel during the recovery period.
- Present an orderly course of action for restoring critical computing capability to Cornerstone and for maintaining and/or restoring client service and support.

Cornerstone performs site-to-site replication of data to protect client data in the event of a disaster. There are two dedicated disaster recovery sites distant from each of the production data centers. Disaster recovery testing is performed annually at each DR site.

Data is safeguarded with real-time replication and/or log shipped databases. This provides for low latency (1-hour recovery point objective) of client transaction data. Disaster recovery servers are located in the Ashburn, VA Equinox facility and in the SunGard facility in Elland, UK. Database and file servers receive a constant real-time stream of updated information from the production data centers either by using software and/or storage hardware based data replication. All other servers required for operation have been built, configured, and tested in advance to ensure they are ready at TOD (Time of Disaster).

Cornerstone is responsible for data backup and recovery. Data is a primary concern for Cornerstone and its clients, 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.

TLMS

SuccessFactors has developed and maintains 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 Office of Personnel Management (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 datacenter 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 IPSec VPNtunnels.

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

Continuity of Operations

The Memphis Data Center (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.

In the event the MDC becomes inoperable, network operations would be relocated to the Martinsburg IRS facility in Martinsburg, W.V., in accordance with the EBS Disaster Recovery

Plan (EBSDRP). This facility employs a "warm site" strategy for recovery of network operations. The *Network Operations, Infrastructure Operations & Engineering Team* is responsible for all the MDC network devices' and servers' hardware, operating systems, and both open source and commercial-off-the-shelf (COTS) application installs and configuration. Since the Martinsburg site is mostly a duplicate system of the MDC site, recovery operations generally involve updating the Martinsburg domain name server (DNS) to point from the MDC systems to the Martinsburg systems.

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.

Complementary User Entity Controls

EBS's controls related to the HRConnect Services system cover only a portion of overall internal control for each user entity of EBS. It is not feasible for the control objectives related to HRConnect Services to be achieved solely by EBS. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with EBS's controls and the related tests and results described in section IV of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

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

Control Objective 3: Access to Computerized Applications and Sensitive Information

- Access to the systems to users who have been vetted by their organization's security requirements.
- 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.
- 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 12: Secure Interface Processes

- Client's technical contact tests connectivity from the client's border server to the EBS border server, using Secure Shell (SSH) and Secure File Transfer Protocol (SFTP).

- Recommended but not required: The client's technical contact places the client's border server public key on the EBS border server so that certificate-based authentication can take place.
- Client's technical contact tests file transfers (pushes and pulls) between the client's border server and the EBS border server.

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

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:

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

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

Security Management Controls

Control Objective 1: System Security Plan

Controls provide reasonable assurance that HRConnect Services system security plan and testing of that plan is kept current and in accordance to Federal guidelines.

Control Activities

1. System Security Plans (SSP) are maintained by the HRConnect Cyber Security team and housed within the Treasury FISMA Inventory Management System (TFIMS).
2. A plan of action and milestones (POA&M) is developed and maintained for controls that have been determined through independent assessments to be less than effective.
3. Security Assessment &Authorization for HRConnect is performed every three years (currently expiring September 2019) based on current Treasury Policy 85-01.

Tests of Operating Effectiveness

1. Inspected the System Security Plan (SSP) to determine whether the SSP was prepared in accordance with NIST SP 800-18, Revision 1 *Guide for Developing Security Plans for Federal Information Systems.*
2. Inspected corrective action plans to determine whether the documentation showed sufficient support for the progress and completion of milestones.
3. Inspected the Security Assessment & Authorization (SSA) to determine whether the SSA for HRConnect was conducted every three years based on current Treasury Policy 85-01.

Results of tests

No exceptions noted.

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

Control Objective 2: Security Related Personnel Policies

Controls provide reasonable assurance that Security related personnel policies include hiring practices of background investigations, confidentiality agreements, termination, and transfer procedures including exit interviews which encompass the returning of property, keys, and removal of logical and physical access.

Control Activities

1. Prospective employees and contractors must undergo background investigations.
2. Security related subject matters are regularly emailed to personnel and posted to the internal share drive.
3. New employees receive an onboarding package Users are required to complete Cyber Security Awareness training and sign a Rules of Behavior agreement within 30 days of employment. (See Control Objective 8 for further discussion of Security Awareness training.)
4. Treasury Office of Security Programs maintains physical access and personnel policies.
5. Exit procedures include a Provisioning for Personnel (P4P) form are completed for termination of access privileges within two business days and the return of property.

Tests of Operating Effectiveness

1. Inspected the most recent and approved policies and procedures for background investigations to determine whether they were followed.
2. Inspected security related subject matters to determine whether security related subject matters were regularly emailed to personnel and posted to the internal share drive.
3. Inspected a selection of employee's and contractor's files determine whether new employees receive an onboarding package of information regarding internal security policies prior to their start date.
4. Inspected a selection of employee's and contractor's files to determine whether internal security policies (Rules of Behavior and Cybersecurity Awareness) agreements were signed and dated and to determine whether the Security Awareness training was completed.
5. Inquired of management and inspected documents to determine whether the Treasury Office of Security Programs maintained physical access and personnel policies.
6. Inspected the Exit Procedures to determine whether the procedures agreed to management policy.
7. Inspected a selection of the terminated employees' and contractors' records to determine whether P4P forms were completed.

Results of tests

No exceptions noted.

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

Access Controls

Control Objective 3: Access to Computerized Applications and Sensitive Information

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

Control Activities

HRConnect

1. Access to HRConnect is restricted to users with a valid logon identification and password.
2. Password reset request are initiated from the Forgot your User ID or Password link and facilitated via the Password Management System (PWMS).
3. Access privileges are granted based on the level of access required to support the process (e.g. for HR - processor, specialist). All managers get access to initiate actions. Managers can assign proxies to initiate, approve or initiate and approve actions on their behalf.
4. Bureau/Sub-agency super users are created using forms requiring agency and supervisor approval. These forms are e-mailed to the Customer Solutions Team E- mail box.
5. User accounts are deactivated via the Personnel Action Requests (PAR) process for employees terminating. User ID's that have been deactivated due to termination are automatically locked.
6. Super users are analyzed quarterly to determine which users are no longer needed due to termination or transfer.
7. Health check reports are generated twice a month. The health check consists of several reports:
    a. User accounts with duplicate email addresses. This is reviewed by Customer Solutions.
    b. Positions that are encumbered by more than one employee. This is forwarded to the agency for review.
    c. Active employees reporting to inactive positions. This is forwarded to the agencies for review.
    d. Separated employees that need to be removed from the PAR Approving Officials table, and name changes to update the PAR Approving Officials table. This is reviewed by Customer Solutions.

inCompass

1. Access to inCompass is restricted to users with a valid logon identification and password.
2. Password reset requests are facilitated through automated email notification.

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

3. Daily reports are provided 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.
4. Privilege level access is granted using access control forms.

InTime

1. New users, transfers and terminations are established through HRConnect daily export file.
2. Temporary passwords are sent via email to new users requesting them to change their passwords. The newly established passwords are valid for specified number of days and then required to be changed.
3. Invalid login attempts are limited upon which the user is locked out.
4. Various audit functions are performed via application menu of audits available.
5. Treasury privilege user access granted after completing access request form and obtaining supervisor approval.
6. DOL privilege user access categories include several levels of access.

Remote Access

1. Remote access to the Departmental Offices network is granted after the employee's supervisor sends an email authorizing remote access. Once remote access is granted the employee/contractor can remotely access the same systems they access at their duty station.
2. Information provided in the authorizing email is used for completing a P4P form.

Other

1. Data Center hard drives, storage devices, Storage Area Network storage devices, 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.
2. Individuals with access to Personally Identifiable Information (PII) are required to sign an HR Connect Program Office (HRCPO) Agreement to Safeguard Sensitive Data.
3. PII data is stored in HRConnect. The data is encrypted at rest and in transit. If there is a PII breach or possible breach the issue is reported to the HRCPO ISSM as soon as possible.
4. Privilege user accounts in production are controlled by strong passwords. Passwords are locked after inactivity and are manually deleted by the Helpdesk.
5. Border server access is granted for users completing an HRConnect User Access Request form.

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

User Acceptance Testing

1. Testers complete an EBS HRC Agreement to Safeguard Sensitive Data as a part of the UAT process. The documents are stored on the J:\ drive in the folder that corresponds to the release.

Complementary User Entity Controls

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

1. Access to the systems to users who have been vetted by their organization's security requirements.
2. 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.
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).

Tests of Operating Effectiveness

1. Inspected password control configuration to determine whether the configuration agreed with management policy and procedures.
2. Observed an executed password reset to determine whether reset process agreed with management policy and procedures.
3. Inspected relevant policies and procedures to determine whether segregation of duties and least privilege controls were in place.
4. Inspected a selected sample of HRConnect users to determine whether access privileges were appropriate for job title and responsibilities.
5. Inspected relevant policies and procedures to determine whether access privileges of a Super User and Normal User were defined.
6. Inspected a selected sample of HRConnect users to determine whether users completed Bureau / Sub-agency Super User forms.
7. Inspected the Super User quarterly review to determine whether they agreed with management policy.
8. Inspected the Health Check Reports to determine whether the reports were generated twice a month and reviewed by the Customer Solutions Section.
9. Inspected a selection of access request forms to determine whether remote access to the Departmental Offices Network was granted after the employee's supervisor sent an email authorizing remote access.
10. Inspected a selection of P4P forms to determine whether information provided in the authorizing email was used for completing a P4P form.

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

11. Inquired of IT management and inspected polices to determine whether Data Center's hard drives, storage devices, Storage Area Network (SAN) storage devices, removable devices were required to be pulverized and were not traded-in to the vendor or disposed of as being surplus.
12. Inspected a selected sample of users with PII access to determine whether the users completed records and signed HRCPO Agreement to Safeguard Sensitive Data.
13. Inquired of IT management and inspected evidence to determine whether data was encrypted at rest and in transit and to determine whether PII breaches were reported to the proper organizations.
14. Inspected PeopleSoft password configuration to determine whether privileged user accounts in HRConnect Production Environment (HR PROD) were protected by strong authenticator management controls.
15. Inspected a selected sample of border server access users to determine whether users completed HRConnect User Access Request Form.
16. Inspected a selected sample EBS HRC Agreements to Safe Sensitive Data to determine whether testers complete the Agreement as a part of the User Acceptance Testing (UAT) process.

Results of tests

No exceptions noted.

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

Configuration Management Controls

Control Objective 4: 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 System Development Life Cycle methodology (SDLC).

Control Activities

1. Updated SDLC is reviewed, approved, and updated as needed.
2. Change requests are managed and controlled through ClearQuest change management software.
3. Functional design documents are used to document the functional design of the approved change request.
4. Review board meeting regularly to review and approve change request functional design documents.

Tests of Operating Effectiveness

1. Inspected the SDLC to determine whether it was reviewed, approved, and updated.
2. Inspected a selected sample of HRConnect change requests to determine whether the change requests were managed and controlled through Clear Quest.
3. Inspected a functional design document (FDD) to determine whether the FDDs were used to document the functional design of the approved change request.
4. Inspected a selected sample of HRConnect change requests to determine whether change requests were reviewed and approved in review board meetings.

Results of tests

No exceptions noted.

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

Control Objective 5: Development and Maintenance Activities for HRConnect Applications and Related Software

Controls provide reasonable assurance that HRConnect applications and related software development and maintenance activities are authorized, documented, tested, and approved.

Control Activities

1. Proposed change requests (CRs) are submitted to the Intake team. Proposed change requests are reviewed weekly with functional analysts and developers. Recommendations are then shared with the management team for approval.
2. If recommended to move forward a Business Requirement Document and Level of Effort are created and shared with the customer.
3. CRs are discussed in the monthly configuration control board meeting and feedback is requested from the customers.
4. If the CR is recommended/selected alternative impacts, both, positive or negative are documented if appropriate, and the functional design document (FDD) is approved by the Director of HRConnect Products and the functional architect.
5. If the CR Level of Effort (LOE) is less than 40 hours, (data only update, one-time script, minor text changes to pages, emails, etc.) a FDD and/or Test Design Document (TDD) may not be required. A waiver is submitted and documented for approval.
6. Developer performs a TDD review to walk through the changes and impact based on the FDD. TDD are a working document and are completed at the end of development.
7. Once the development and technical documentation is complete, each CR must have a functional design document, technical design document 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.
8. Each stage/lifecycle is separate for purposes of creating an independent process (development, testing, internal validation, and customer user acceptance). At the end of the cycle (whether internal or customer acceptance) approval is performed for the changes made.

Tests of Operating Effectiveness

1. Inquired with HRConnect management to determine whether proposed change requests (CRs) were submitted to the Intake team; proposed change requests were reviewed weekly with functional analysts and developers, and recommendations were shared with the management team for approval.
2. Inspected a selection of Business Requirement Document (BRD) and Level of Effort (LOE) documents to determine whether BRDs and LOEs were created and shared with the customer if it's recommended to move forward with changes.

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

3. Inspected monthly board meeting minutes to determine whether CRs were discussed in the monthly configuration control board (CCB) meeting and feedback was requested from the customers.
4. Inspected supporting documentation to determine whether alternative impacts (positive or negative) was documented and the FDD was approved by the Director of HRConnect Products and the functional architect. (see exception noted below)
5. Inspected waivers to determine whether the waivers were submitted and documented for approval when a FDD and/or TDD was not required because the CR LOE was less than 40 hours.
6. Inspected a selected sample of TDD to determine whether developers perform TDD reviews to walk through the changes and impact based on the FDD.
7. Inspected a selected sample of CR to determine whether CRs contained the appropriate development and technical documentation.
8. Inspected a selected sample of CR to determine whether approvals are performed for the changes made at the end of the stage/lifecycle.

Results of tests

Exceptions Noted: For 5 of the 5 FDDs tested, the appropriate officials did not sign the documents.

No other exceptions noted.

Management Comment: Treasury is reviewing the HRConnect Control Objective 5: Development and Maintenance Activities for HRConnect Applications and Related Software process to ensure the FDDs are signed with the appropriate signatures going forward.

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

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.

Control Activities

1. Manual security inspection is performed on In-Time firewalls.
2. Vulnerability scans are conducted monthly.
3. Penetration testing occurs annually.
4. Vulnerability Executive Summary spreadsheet tracks all monthly scans that are conducted by EBS cyber engineers.

Tests of Operating Effectiveness

1. Inspected a selected sample of manual security inspections to determine whether the inspections were performed on the In-Time firewalls.
2. Inspected vulnerability scans to determine whether vulnerability scans were conducted monthly.
3. Inspected the results of the penetration to determine whether penetration testing occurred annually.
4. Inspected the Vulnerability Executive Summary spreadsheets to determine whether the spreadsheets tracked all monthly scans that were conducted by EBS cyber engineers.

Results of tests

No exceptions noted.

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

Control Objective 7: Physical Access Policies

Physical access by all employees and visitors to facilities and data centers and systems is appropriately authorized.

Control Activities

EBS location

1. Security guard located within lobby of the build requiring signature of guest and escort by EBS employee. Signature is maintained in hard copy log book at the guard station.
2. Access to floors within the building is controlled using pre-numbered personal identity verification (PIV) cards. PIV cards control access to facilities as well as the physical access of computer equipment.

PIV Cards

1. Each employee and contractor is issued a PIV card after the appropriate security approval.
2. At the time of onboarding, a P4P form is completed, which is used to verify the supervisor's position and employee's position. If access is needed for additional hours outside of regular business hours, the supervisor must stipulate this in the request. If the person is a contractor, a contractor suitability email from the Office of Security Program stating that the contractor is cleared for building.
3. An employee transferring positions within Treasury that necessitate new/altered building access is communicated via email from the employee manager/supervisor to "Main Treasury", who verifies the change and forwards the request to the appropriate building access point of contact for processing
4. Employees terminating employment return their-PIV card which is then deactivated.

Tests of Operating Effectiveness

1. Inspected the lobby to determine whether the security guard located within the lobby of building required signatures of a guests and were escorted by an EBS employee.
2. Inspected PIV cards to determine whether access to floors within the building was controlled using PIV cards.
3. Inspected supporting documentation to determine whether each employee and contractor was issued a PIV card after the appropriate security approval.
4. Inspected physical assessments to determine whether the assessments were performed every three years as disclosed in the Security Risk Assessment.
5. Inspected data center site survey to determine whether site surveys were performed every three years by IRS.

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

Results of tests

No exceptions noted.

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

Control Objective 8: Compliance with Education, and Training Policies

Controls provide reasonable assurance that Employees comply with code of ethics and conflict of interest standards. Education and training programs are in place to ensure that employees understand their responsibilities.

Control Activities

1. Annual IT Security and Privacy awareness and Ethics training is required. Specialized training is based on roles within the HRConnect.
2. HRCPO offers Application specific training to HRConnect customers.

Tests of Operating Effectiveness

1. Inspected documentation to determine whether annual IT Security, Privacy Awareness, and Ethics training was required and whether specialized training was based on roles within HRConnect.
2. Inspected a list of application specific training to determine whether application specific training was offered for HRConnect.

Results of tests

No exceptions noted.

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

Control Objective 9: 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.

Control Activities

1. Customer surveys are performed of customers by the Office of Personnel and Management
2. Annual customer service surveys are performed of each customer.
3. Results of the surveys are discussed during the monthly configuration control board meetings.
4. Changes to agreements are documented using United States Government Interagency Agreement (IAA) form as well as product specific addendums.

Tests of Operating Effectiveness

1. Inspected evidence to determine whether customer service surveys were performed of customers by the Office of Personnel and Management.
2. Inspected evidence to determine whether annual surveys for each customer were performed.
3. Inspected evidence to determine whether the results of polls and surveys are discussed during the monthly configuration control board meetings.
4. Inquired with HRConnect management and inspected IAA forms to determine whether changes to agreements were documented using forms IAA as well as product specific addendums.

Results of tests

No exceptions noted.

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

Control Objective 10: Corrective Action Response Plans

Controls provide reasonable assurance that A corrective action process is in place to address findings noted from all security audits and reviews of IT systems, components, and operations.

Control Activities

1. Plan of Action and Milestone (POA&M) are used to identify any findings, deficiencies or weaknesses noted in audits and security assessments. All POA&M's are tracked in TFIMS. Corrective actions are reviewed to determine whether the recommendation was properly implemented before the POA&M could be closed.

Tests of Operating Effectiveness

1. Inspected POA&Ms to determine whether the POA&M process was compliant with NIST SP 800-37, Revision 1.

Results of tests

No exceptions noted.

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

Control Objective 11: Accuracy Testing Methods

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

Control Activities

HRConnect to WebTA

1. All data transmitted to InTime are contained in fixed length, sequential 'flat' files.
2. Employee Profile and Timesheet Profile data are extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of these file formats
3. Accounting- Common Governmentwide Accounting Classification Structure (CGAC) data are extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of this file formats.
4. Accounting-CGAC data are extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of this file formats.
5. Leave Balances data is extracted and transmitted bi-weekly from HRConnect.
6. Organization Structure data is extracted and transmitted only when needed for description or status (active/inactive) changes to the departments contained in the structure.
7. Structural changes (parent/child) that result in a new effective dated tree require the entire Organization Structure are transmitted for replacement within WebTA
8. Any error with a timesheet during the export result in the timesheet being flagged as "action required" and the timesheet employee's supervisor being notified. All system administrators are alerted to any failed timesheets via the InTime notification system. A single timesheet failure is not prevented the rest of the timesheets from processing or being transmitted.

Automated InTime Interfaces

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

DOL Accounting Interface

1. 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.
2. EBS receives DOL's NFC files after payroll is run every Monday at 6 a.m.

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

HRConnect to inCompass Interface

1. Data feed error report is generated Monday - Friday for all customers to determine if there are any interface errors.
2. Follow-up communication with customers regarding interface variances is via email.
3. Successful data interface is evidenced by customer email notification showing data feed log.
4. User and organizational unit files are placed on the border server for customers to retrieve.

Tests of Operating Effectiveness

1. Observed IT Specialist to determine whether 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 to determine whether 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 to determine whether Accounting-CGAC data was extracted and transmitted daily from HRConnect for new hires, separations, and any changes to the data elements of this file formats.
4. Inspected a selection of Leave Balances data from InTime to determine whether Leave Balances data was extracted and transmitted on an ad-hoc basis from HRConnect and whether Group 6-NFC Leave Balance Interface TDD captures the process.
5. Inspected a selection of Organization Structure Data from InTime to determine whether the data was extracted and transmitted only when needed for description or status (active/inactive) changes to the departments contained in the structure.
6. Inspected a selection of Organization Structure changes from HRConnect to determine whether 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 selected sample of time sheets to determine whether a process was in place to identify and follow up on timesheet errors.
8. Inspected the interface schedule to determine whether interfaces are regularly scheduled for designated times throughout the week.
9. Inspected the log of interfaces within InTime to determine whether a log of the interfaces is captured within InTime.
10. Inspected emails to determine whether emails are generated from InTime indicating successful transmission or exceptions.
11. Inspected the Accounting Interface Requirements Summary Document to determine whether 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.

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

12. Inspected records of EBS receipt of DOL's NFC files to determine whether EBS receives DOL's NFC files after payroll is run every Monday at 6 a.m.
13. Inspected data feed error reports to determine whether a data feed error report was generated Monday - Friday for all customers about interface errors.
14. Inspected emails to determine whether customers follow up was conducted on interface variances.
15. Inspected a selection of customer email notifications to determine whether a successful data interface was evidenced by customer email notification showing data feed log.
16. Inspected access request forms to determine whether customers were properly authorized to retrieved files from the border server.

Results of tests

No exceptions noted.

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

Control Objective 12: Secure Interface Processes

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

Control Activities

1. EBS Deployment Team reviews the interface and EBS Security Team approves the establishment of the new interface. An updated is required every three years.
2. EBS Deployment Team provides the client's technical contact with an EBS Access Request Form.
3. EBS Development 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 client's technical contact.
4. 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.
5. 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.

Complementary User Entity Controls

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

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

Tests of Operating Effectiveness

1. Inspected a selected sample of new interface documentation to determine whether the Deployment Team reviewed the documentation and whether it was approved by the Security Team.
2. Inspected a selection of EBS Access Request Forms to determine whether the Deployment Team provided the client's technical contact with an EBS Access Request Form.
3. Inspected a selection of technical contacts to determine whether the EBS TA team provided the connectivity information to the client's technical contact.

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

4. Inspected emails and screenshots to determine whether the client's technical contact tested connectivity from the client's border server to the EBS border server, using SSH and SFTP.
5. Observed an administrator demonstrate a SSH session on the EBS border server to determine whether the client's technical contact places the client's border server public key on the EBS border server so that certificate-based authentication took place.
6. Inspected emails documenting tests file transfers (pushes and pulls) between the client's border server and the EBS border server to determine whether the client's technical contact tested file transfers (pushes and pulls) between the client's border server and the EBS border server.
7. Inspected supporting documentation for a selection of CQ TA Work Orders to determine whether 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.
8. Inspected a CQ TA Work Order to determine whether 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.

Results of tests

No exceptions noted.

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

Control Objective 13: Subservice Organizations

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

Control Activities

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 reporting of HRConnect systems.

Tests of Operating Effectiveness

1. Inspected supporting documentations to determine whether HRConnect management reviewed the results of its subservice organizations' SSAE 18 examination within 3 months of the reports being issued.
2. Inspected supporting documentations to determine whether HRConnect management monitored and documented changes to the subservice organizations' audit results that impacted the HRConnect systems and whether these documentations were signed off by the system owner after EBS receives NFC's SSAE 18 examination report or control related documentation provided by subservice organizations.

Results of tests

Exception noted:

The subservice organization designed its service with the assumption that certain controls would be implemented by EBS in order to achieve certain controls objectives that cannot be achieved by the subservice organization alone.

Sufficient documentation was not provided to indicate that EBS monitored its subservice organizations' Statement on Standards for Attestation Engagements (SSAE) No. 18 report or other control related documentation provided by subservice organizations. As a result, controls were not operating effectively to achieve the control objective 13: Controls provide reasonable assurance that EBS monitors subservice organizations and test for compliances with complementary user entity controls.

EBS did not maintain evidence of monitoring and testing of subservice complementary user entity controls.

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

Without accurate records of monitoring and testing of subservice complementary user entity controls, EBS cannot demonstrate through its documentation whether it properly performed the complementary user entity controls and accordingly cannot demonstrate through its documentation whether the subservice controls operated as intended.

Management's Response: Treasury is reviewing the HRConnect Control Objective 13: Monitor and Control Subservice Organizations process to ensure it meets the control going forward.

V. OTHER INFORMATION PROVIDED BY ENTERPRISE BUSINESS SOLUTIONS

Contingency Planning

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 11, 2016. The most recent test of the Contingency Plan and Disaster Recovery Exercises (DRE) was conducted on May 11, 2016; EBS plans to file the After Action Report and Lessons Learn documentation following this test.

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, and 2016. 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 HRC, the COOP plan to recover the system to IRS Memphis, TN data center facility via the IRS Martinsburg data center).

The Recovery Time Objective (RTO) is 72 hours and Recovery Point Objective (RPO) is one (1) hour. If the plan is to be activated, the Disaster Recovery Coordinator notifies the ISSM, the Customer Solutions Team Leader, and the Technical Architecture Team and inform 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. HRC has developed a Business Impact Analysis (BIA) as of January 26, 2015 version 1.0 and the "HRC Disaster Recovery Plan - May 11, 2016" to support the Recovery Time Objective (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 Business Impact Analysis 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
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 HRC the COOP Plan to recover the system to IRS Memphis, TN data center facility, IRS Martinsburg, Customer Solutions (customers' notification), Treasury BFS TIC, Cisco, EMC SAN, IRS Telecom, Bureau of Fiscal Services (BFS) Bureau of Public Debt (BPD) for testing, Business Intelligence systems (WA RS), R&D, etc.).

EBS tests the contingency plan with the alternate processing site. The IRS Martinsburg Computing Center (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 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 HRC 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 stand-by database.

The Memphis and Martinsburg Data Centers Teams are responsible for providing key services at the Memphis and Martinsburg Data Center including enterprise network infrastructure, Storage Area Network (SAN) and the data backup services in support of the HRConnect production environment at Memphis and Martinsburg. The SAN is not part of the HRC accreditation boundary per Technical Architecture team.

The alternate storage site for the Human Resources Connect System (HRC) in IRS' Memphis TN (MEM) facility is the IRS Martinsburg WVA data center facility. The IRS Martinsburg WVA 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 WVA data center facility. The HRC area at IRS Martinsburg WVA data center facility is under lease exclusively to Treasury Information Operations (IO) and operated by Treasury Information Operations (IO) as the HRC 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. Full and partial backups staggered with files going to netbackup and thence 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 one (1) hour RPO, HRConnect uses the Oracle Data Guard, 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 Martinsburg Computing Center (MTB) in Martinsburg, WV. All transaction logs are sent from MEM (primary site) to MTB (alternate site DR facility)

every 20 mins 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 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, DataDomain appliances. The system executes and manages a series of scripts to back up data files, 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 Martinsburg Computing Center (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. Data Guard 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 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