Audit Report

OIG-22-044

FINANCIAL MANAGEMENT

Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2021, to June 30, 2022

September 28, 2022

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

September 28, 2022

MEMORANDUM FOR NICOLAOS B. TOTTEN
ASSOCIATE CHIEF INFORMATION OFFICER
ENTERPRISE APPLICATIONS

FROM: Ade O. Bankole /s/
Director, Financial Statement Audits

SUBJECT: Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2021 to June 30, 2022

We hereby transmit the attached subject report. Under a contract monitored by our office, Saggar & Rosenberg, P.C. (S&R), a certified independent public accounting firm, examined the Enterprise Applications' (Enterprise Apps) 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 the description of controls provided by Enterprise Apps, management's written assertion, and S&R's independent service auditor's report. The contract required that the examination be performed in accordance with U.S. generally accepted government auditing standards and the attestation standards established by the American Institute of Certified Public Accountants.

In its examination, S&R found in all material respects:

- the description fairly presents the HRConnect system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022;

- 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 July 1, 2021 to June 30, 2022, and subservice organizations and user entities applied the complementary user entity controls assumed in the design of Enterprise Apps' controls throughout the period July 1, 2021 to June 30, 2022; and

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2021 to June 30, 2022, if complementary subservice organizations and user entity controls assumed in the design of Enterprise Apps' controls, operated effectively throughout the period July 1, 2021 to June 30, 2022.

In connection with the contract, we reviewed S&R'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 Enterprise Apps' description of controls, the suitability of the design of these controls and the operating effectiveness of controls tested. S&R is responsible for the attached independent service auditor's report dated September 23, 2022, and the conclusions expressed therein. However, our review disclosed no instances where S&R did not comply, in all material respects, with generally accepted government auditing standards.

If you wish to discuss this report, please contact me at (202) 927-5329, or a member of your staff may contact Mark S. Levitt, Manager, Financial Statement Audits, at (202) 927-5076.

Attachment

Department of the Treasury
Enterprise Applications

Report on the Enterprise Applications' Description of its HRConnect System and the Suitability of the Design and Operating Effectiveness of Its Controls

For the Period
July 1, 2021 to June 30, 2022

Table of Contents

I: INDEPENDENT SERVICE AUDITOR'S REPORT PROVIDED BY SAGGAR & ROSENBERG, P.C. (S&R)

SAGGAR & ROSENBERG, P.C.
Assurance • Tax • Consulting

Independent Service Auditor's Report

Deputy Inspector General, Department of the Treasury
Associate Chief Information Officer, Enterprise Applications

Scope

We have examined Department of the Treasury, Enterprise Applications' (Enterprise Apps) description of its HRConnect system for processing user entities' human resource transactions throughout the period July 1, 2021 to June 30, 2022 (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 Applications" (assertion). The controls and control objectives included in the description are those that Enterprise Apps 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.

Enterprise Apps uses subservice organizations identified in Section III and IV to perform hosting services. The subservice organizations include Oracle Cloud Infrastructure's Infrastructure as a Service (OCI IaaS) and National Finance Center (NFC). The description includes only the control objectives and related controls of Enterprise Apps and excludes the control objectives and related controls of subservice organizations. The description also indicates that certain control objectives specified by Enterprise Apps can be achieved only if complementary subservice organization controls assumed in the design of Enterprise Apps's controls are suitably designed and operating effectively, along with the related controls at Enterprise Apps. Our examination did not extend to controls of subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Enterprise Apps's controls are suitably designed and operating effectively, along with related controls at Enterprise Apps. 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, Enterprise Apps 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. Enterprise Apps is responsible for preparing the description and 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 (AICPA) and 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 July 1, 2021 to June 30, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 stated in the description, 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 of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in Enterprise Apps's assertion in Section II of this report:

- The description fairly presents the HRConnect system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022;
- 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 July 1, 2021 to June 30, 2022, and subservice organizations and user entities applied the complementary controls assumed in the design of Enterprise Apps’s controls throughout the period July 1, 2021 to June 30, 2022; and
- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2021 to June 30, 2022, if complementary subservice organizations and user entity controls, assumed in the design of Enterprise Apps’s controls, operated effectively throughout the period July 1, 2021 to June 30, 2022.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of Enterprise Apps, user entities of Enterprise Apps's HRConnect system during some or all of the period July 1, 2021 to June 30, 2022, 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.

Saggar & Rosenberg, P.C.

Rockville, MD
September 23, 2022

II: MANAGEMENT ASSERTIONS PROVIDED BY ENTERPRISE APPLICATIONS

September 23, 2022

Enterprise Applications' Assertion

We have prepared the description of Enterprise Applications' HRConnect System entitled "Description of Controls Provided by Enterprise Applications" for Treasury's enterprise human resources system processing user entities' transactions throughout the period July 1, 2021 to June 30, 2022 (description) for user entities of the system during some or all of the period July 1, 2021 to June 30, 2022, 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.

Entrprise Applications' uses a subservice organizations for payroll services and for their HR system platform, provided by USDA National Finance Center (NFC) and Oracle respectively. The description includes only the control objectives and related controls of Enterprise Applications and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls atthe service organization. The description does not extend to controls of the subservice organization.

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 Applications' 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 July 1, 2021 to June 30, 2022, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

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

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

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

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

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

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

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

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

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

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

b. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2021 to June 30, 2022, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Enterprise Apps's controls throughout the period July 1, 2021 to June 30, 2022. The criteria we used in making this assertion were that:

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

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

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

Sincerely,

Nicolaos B. Totten

Digitally signed by Nicolaos B. Totten
Date: 2022.09.23 15:38:37 -04'00'

Nicolaos B. Totten
Associate Chief Information Officer
Enterprise Applications
U.S. Department of the Treasury

III: DESCRIPTION OF CONTROLS PROVIDED BY ENTERPRISE APPLICATIONS

OVERVIEW OF OPERATIONS

This examination only covers the products and services provided by the Enterprise Applications (Enterprise Apps) relating to the HRConnect system. Enterprise Apps is one of the organizations that Office of Personnel Management (OPM) has authorized to manage a federal Human Resources Line of Business (HRLOB). As an HRLOB Shared Services Provider, the HRConnect System is used by all Treasury bureaus and several other government agencies (over 34 entities) with over 230,000 employees and contractors in total.

The HRConnect System is the Department of the Treasury's (Treasury) enterprise human resources system. The HRConnect System is based on a combination of a web-based solution built on PeopleSoft commercial-off-the-shelf (COTS) software, which constitutes as a Platform as a Service (PaaS) platforms (e.g. general support systems of the HRConnect enclave domains of operating systems and database management support systems (DBMS), and support software).

The HRConnect System transforms core back-office Human Resources (HR) functions, moving them from a processing-centric capability to a strategic-centric capability enabled through its commercial software underpinning. Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers and employees.

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

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

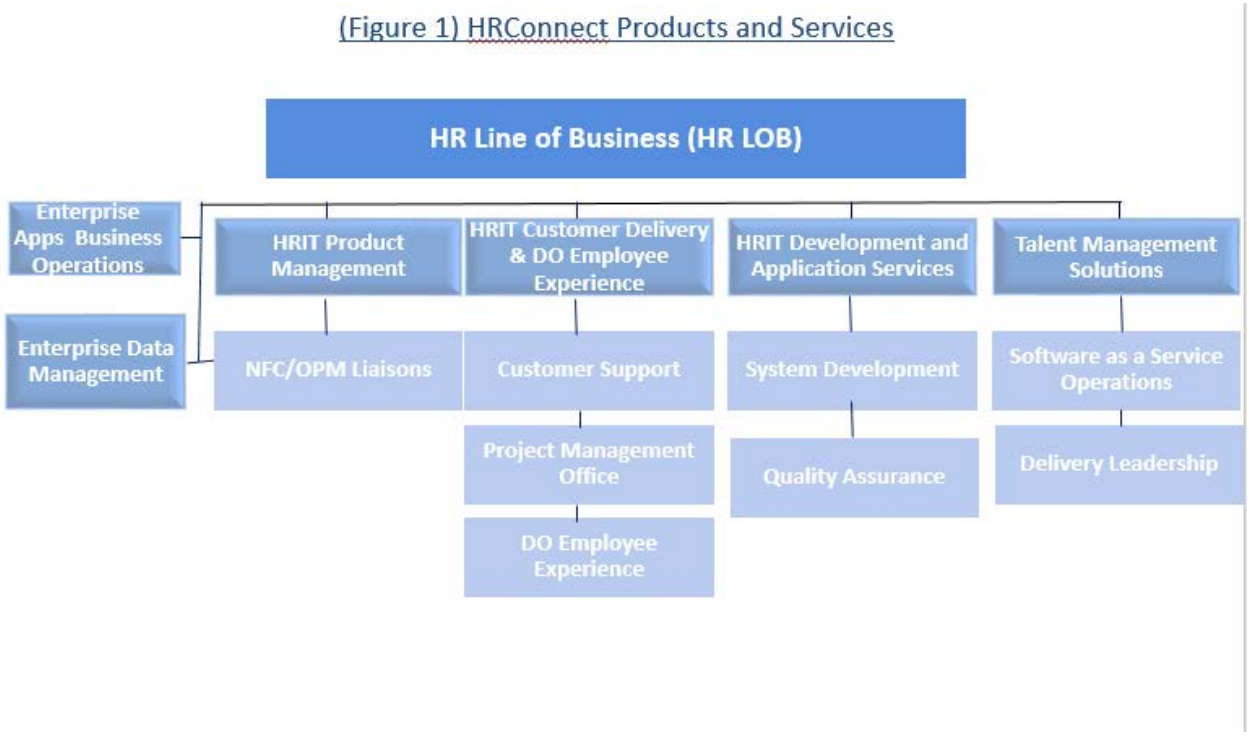


Figure 1: HRConnect Products and Services Organizational Structure

HRConnect

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

Additionally, self-service components of the software fundamentally transform the standard government HR service delivery model, putting additional information, services, and processes (i.e., personal data, position management, requests for personnel action, recruitment, reporting, etc.) directly in the hands of managers, employees, and HR professionals. HRConnect features/functionality are included in Table 1 (below):

List of HRConnect Products and Services:

HRConnect System Features/Functionality	
Automated Password Management	Treasury HRConnect guides new users through the initial registration process and assigns a User ID and temporary password. Forgotten IDs/Passwords, as well as Need to Change Passwords, are also managed in the same secure environment. Help Desk intervention is not generally required, except for unlocking user accounts.
Manager, Employee and HR Self Service	Personnel Action Requests (the electronic equivalent of an SF-52) may be initiated online by Managers (and/or their Proxies or Detail Managers) using Manager Self Service. HR staff can process or initiate a full suite OPM-approved transactions (in 55 different action/reason categories) in HRConnect. A Mass Update Module feature is also available to HR to easily process many similar requests with one transaction (realignments, reassignments, etc.). Employees may initiate 9 actions and 19 updates to personal information, including address, phone number, and emergency contact information as well as the ability to request to retire or resign. In addition, users may view personal information, benefits, leave balances, and salary, performance and award history.
Personnel Action Requests (PARs)	PARs may be initiated by Managers, their Proxies, Detail Managers, and HR specialists. HR staff can process a full suite of OPM-approved transactions (over 150 PAR actions) in HRConnect.
Payroll Interface and Error Correction	Treasury HRConnect features a robust daily bi-directional interface, which transmits personnel, position, and payroll information to the National Finance Center (NFC), Treasury's payroll partner. The reverse interface provides all applied actions, historical corrections, and NFC-generated automatic actions (within-grade increases, etc.) back to Treasury HR System (HRConnect). This interface allows for error correction (SINQ's) directly in Treasury HRConnect and delivers a comprehensive match solution to keep data synchronized.
Payroll Processing	Treasury HRLOB partners with the NFC to perform all the payroll related processes as well as other services normally associated with the payroll.
Benefits Services	Treasury HRLOB's HR processing partner, Fiscal Service Administrative Resource Center, provides staff to support the administration of benefits (retirement, life insurance, health insurance, Thrift Savings Plan, Long Term Care Insurance Program, Flexible Spending Account, retirement annuity calculations, and Employee Assistance Program). This is a separate service that Treasury customers may request. Additionally, HRConnect provides convenient access to helpful links to a variety of information, including National Finance center Employee Personal Page, tax calculator, salary tables, TSP information, safety and health programs, and more.
Interfaces to Agency/Bureau and other service provider systems	Treasury HRConnect provides data feeds to multiple Agency/Bureau systems, including data warehouses, Learning Management Systems, and other service providers. These interfaces can be accomplished through a various technical process.

HRConnect System Features/Functionality	
Workflow and Worklists	Managers and HR specialists are able to access actions directed to them online for authorization or approval using workflow and worklists. Personnel and other actions are moved automatically through a configurable workflow that includes management authorizations and HR approvals. A sophisticated set of routing rules can be invoked to direct actions by type or location to HR specialists in that category of action (e.g., Suspensions to ER specialists).
Position Management	Treasury HRConnect provides the ability to manage workforce through position creation, allocation, budgeting, obligation, and incumbency tracking, such as Position Wizard.
Position Budget Management	Position Budget Management (PBM) allows a budgeting office to designate the distinct account code or codes to which the payroll expenses for a specific position will be charged. This function prevents the use of positions for which no account code has been assigned and automates the assignment of new codes as well as the removal of inactivated codes. Automated workflow and system-generated notifications, as well as standard reports and the inclusion of position budget data in the Workforce Analytics reporting system, enable budget analysts to monitor the position budget status of their assigned organizational units and to take actions as needed.
Mass Processing	At times, managers may wish to initiate mass actions that impact a group of employees. Manager Self Service efficiently handles mass awards and mass realignments.
Payroll Documents	HR specialists have the ability to initiate 30 different payroll documents (e.g., federal, state and local taxes, allotments, health insurance, direct deposits, and health benefits, including several non-federal documents) directly within HRConnect. Afterwards, the HR specialists will transmit these documents into NFC.
Emergency Contacts	Employees can input an extensive list of emergency contacts. Each emergency contact includes the contact name, address, phone number(s), and relationship to the employee. This information can be accessed and updated at any time, and reports are available to Managers and HR professionals.
Awards Administration	Managers and HR employees may initiate various types of awards (on-the-spot, cash, time-off, etc.) for direct-reporting employees as well as others in the organization. Bureaus can elect to require optional data fields (e.g., accounting code). Administrators have the ability to specify award codes and limits applicable to their agency that are available in a list for managers to initiate and select. This feature includes the ability to initiate mass award actions for many employees.
Separating Employee and Contractor Clearance (SEC/SCC)	Treasury HRConnect allows online management to initiate the process of clearing an employee who is separating (e.g., securing issued equipment, security passes, credentials, etc.).
Drug Test Tracking	Treasury HRConnect provides a way to track the drug testing information.
Employee and Labor Relations, and Third-Party Case Tracking	Treasury HRConnect provides for tracking of disciplinary cases, grievance cases, and third party (arbitration, etc.) cases. Also allows for tracking negotiation processes between bargaining units and management.
Financial Disclosure Tracking and Reporting	Treasury HRConnect provides the ability to track employees required to submit Form 278 and 450 financial disclosure forms.

HRConnect System Features/Functionality	
FAIR Act Reporting	Treasury HRConnect provides the creation and submission of OMB-compliant FAIR Act reports.
SF-50's	Treasury HRConnect provides the capability for employees and HR professionals to access, view, and print SF-50's online, including required email notification to employees of the availability of their SF-50's.
Automated Email Notifications	Treasury HRConnect automatically sends users notification and reminder emails for NTE dates, SF-50's, worklist items, password expiration, etc.
Continuity of Operations Tracking	Treasury HRConnect provides managers the capability of entering and maintaining Continuity of Operations (COOP) group assignments and the skill sets required for bureau/agency continuation of operations for employees.
System Security	Treasury HRLOB's foundational approach to information security for all IT systems developed and managed by this office is a Defense-In-Depth principle implemented as a layered solution. In short, there are multiple defense strategies for multiple targets or initiatives.
Attachments	Treasury HRConnect provides the ability for Employees, Managers/Proxies, and HR to attach documentation to actions. Attachment functionality allows approving authorities, reviewers, and processors to easily access and review supporting documentation in order to take immediate action, as necessary. Attachments are available in the following areas: personnel actions initiated by HR or Managers; employee updates (e.g., name change, vaccination status); recruit requests; Employee/Labor Relations cases; Health Benefit forms; dependent information; and Separation and Home Leave.
Contractor Management	Treasury HRConnect provide the ability to Contracting Officers to track contracts, task orders, contractors by task order and the type of government furnished equipment supplied to the contractor.
Outside Employment	Treasury HRConnect provides ability for employees to submit requests for outside employment to managers for approval. The system captures information related to the business including business type, business name, and estimated hours.
PIV, Single Sign On (SSO) and Multi-Factor Authentication (MFA)	HRConnect requires multifactor authentication (MFA) by end users through use of PIV (Personal Identity Verification) - badge identification and authentication, Single Sign-On is also available to those end user customers who are joining the Treasury Enterprise Identity Credential and Access Management (TEICAM) Federated Identity Management solution. PIV 2nd factor authentication is passed to the System Security Plan (SSP) Security Assertion Markup Language (SAML) tokens for authentication into HRConnect.

HRConnect Services/Support	
Tier 1 Help Desk Support	Treasury HRLOB partners with the Administrative Resource Center (ARC) to offer Tier 1 Help Desk support. If a customer does not utilize ARC, then the customer is responsible for Tier 1 Help Desk support.
Level 2 and Level 3 Customer Support	Enterprise Apps provides Level 2 and Level 3 Customer support in order to respond to questions and manage the applications. The support includes the following features: • Create and run unique operational reports for the customers • Load data for the customers • Manage the application security requests for privileged users • Manage the bureau access detail configuration • Troubleshoot issues submitted by the customers
Business Process Analysis	Treasury HRConnect's specialists assess the customers' current processes and assist in developing future state processes and a plan for implementation. This is based on an analysis done with the organization to ensure that the processes are in alignment with and best utilize the HRConnect technologies.
Organization Change Management	Treasury HRLOB's Change Management consultants provide guidance, lessons learned, best practices, and variety of processes and techniques to obtain stakeholders' support for change. This is done with the customer to ensure that executive sponsorship and change agents are identified early in the process to ensure success.
System Training	Treasury HRLOB conducts a 3-day course which provides new HR Specialists with hands-on experience on initiating, routing, and processing HR actions upon request. It reviews the common interfaces and provides understanding of how to process, job requisitions; personnel actions requests; SINQs; cancellation and corrections; and workflow requests. In addition to classroom training, the Treasury HRLOB Training Solutions Team is also able to provide webinars, user guides, and more. Additionally, there is an established Customer-based Community of Practice group which meets regularly to educate customers on the various features and functions available.

Table 1: List of Products and Services

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

Control Environment

The control environment is the foundation for all other components of internal control. It provides the discipline and structure, which affect the overall quality of internal control. It influences how objectives are defined and how control activities are structured. Enterprise Apps has established and maintained an environment throughout the organization that sets a positive attitude toward internal control. Through its management, Enterprise Apps has demonstrated a commitment to integrity and ethical values and a commitment to a strong internal control system. Enterprise Apps

has established an organizational structure, assigned responsibility, and delegated authority to achieve its objectives. Enterprise Apps is committed to recruit, develop, and maintain competent employees. Enterprise Apps evaluates performance and holds individuals accountable for their internal control responsibilities.

Enterprise Apps is one of Treasury's Government Shared Services and HRConnect is one of the shared offerings. The mission of Enterprise Apps 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, and 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, which covers the 14 general principles of ethical conduct Codified in 5 C.F.R. Part 2635. Annual privacy training is required by FAR Subpart 24.3 that addresses the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. In addition, all users of information systems must receive awareness training, as required by the Federal Information Security Modernization Act of 2014 (FISMA).

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

Risk Assessment

Enterprise Apps conducts risk assessment 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 responsibilities 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 Enterprise Applications Cybersecurity (EAC) team and high/critical items are brought for review every two weeks by the entire management team. Enterprise Apps Cybersecurity team has a separate Security Assessment and Authorization (SA&A)/risk assessment process including Plan of Action and Milestones (POA&M) management, which data feed into the Enterprise Apps project risk management process. The Enterprise Apps Cybersecurity team performs mini-risk assessments throughout the HRConnect (HRC) lifecycle; for instance high level security impact assessments (SIAs) during the project InTake process and detailed SIAs during the systems change control processes.

Monitoring

Monitoring internal control is a dynamic process that must be adapted continually to manage changing risks. Monitoring of the internal control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the evaluation of the effectiveness of controls over time and promptly resolves the findings of audits and other reviews. Enterprise Apps has established monitoring activities and reacts to events timely with corrective actions. Corrective actions are a necessary complement to control activities in order to achieve objectives.

HRConnect management and supervisory personnel monitor the quality of performance as a normal part of their activities. Management and supervisory personnel inquire of staff and/or review data to ensure the system operates within an effective internal control environment. An example of a key monitoring control is capturing key performance indicators in the monthly Performance Management Review (PMR) report. Enterprise Applications Cybersecurity (EAC) follows the Risk Management Framework (RMF) for maintaining secure FISMA-compliant systems including the recurring myriad continuous monitoring activities throughout the year.

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

Information and Communication

HRConnect offers interoperable, portable, and scalable HR/payroll solutions across the federal space. The HRConnect Core System is an enterprise-wide, web-based HR system, built on PeopleSoft/Oracle commercial-off-the-shelf (COTS) software. HRConnect core functions include: Personnel Action Processing, Payroll Administration, Benefits Administration, Talent Acquisition, Onboarding, Treasury Learning Management, Integrated Talent Management, Employee and Manager Self Service Portal, and HR transaction processing.

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

HRConnect Core is based on the PeopleSoft application. The components are PeopleSoft 9.2, Tools 8.58, Oracle 12C database, WebLogic Web/App servers, and Linux 7 running on X86 servers.

Enterprise Apps has established an effective control environment whereby management assesses the risk facing HRConnect as the Company seeks to achieve its control objectives. Enterprise Apps applies the Risk Management Framework (RMF) to HRConnect, which includes conducting activities related to security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. Enterprise Apps uses Treasury FISMA Inventory Management System (TFIMS) to document this process. A

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 compliant risk assessment was completed as part of the SA&A process.

Enterprise Apps performed a formal risk assessment for the HRConnect system as part of the system authorization process. The assessment consisted of internal and external risks that may potentially impact the system. In consideration of risks from the cloud service provider, Enterprise Apps management verified OCI IaaS' FedRAMP compliance prior to issuing the HRConnect ATO. Enterprise Apps management closely monitor OCI continuous monitoring activities monthly. The activities include the review of system changes, security impacts, any new risks, and remediation actions performed throughout the year by the Oracle. Enterprise Apps has defined HRConnect control objectives to enable the identification of risks and define risk tolerances. In the HRConnect, Enterprise Apps identifies and analyzes risks related to achieve the defined objectives. In addition, Enterprise Apps assesses its risk to be able to respond to significant changes that may impact its internal control system.

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

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

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

Systems and Interfaces

Enterprise Apps uses the following systems and interfaces to provide HRConnect System to federal agencies.

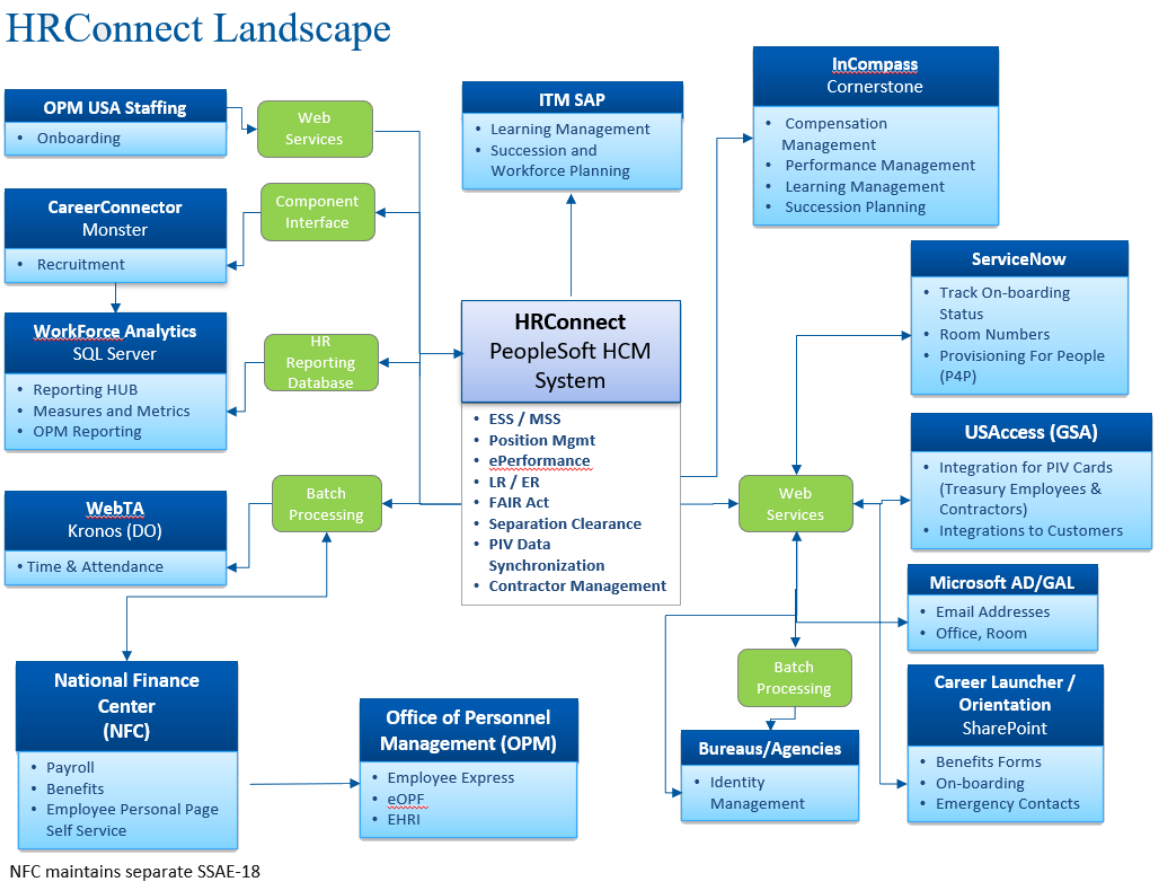


Figure 2: HRConnect Landscape

Note: CareerConnector, Entrance on Duty System (EODS), Integrated Talent Management (ITM) (aside from the interconnection between ITM and HRConnect), and Enterprise Data Management (EDM)/Workforce Analytics systems are not included in this examination.

HRConnect

HRConnect Core is based on the PeopleSoft Human Capital Management application. HRConnect facilitates increased efficiency and overall productivity for its customers. HRConnect Core supports the common HRLOB processes and provides core HR functionality that is interoperable, portable, and scalable. This shared solution provides automated systems that are configurable to each individual organization's needs while providing a single solution across the Department and federal landscape. HRConnect's functions include employee self-service, manager self-service, HR processing, and bi-directional payroll interface. The data that are tracked include, but are not limited to:

- Employee and contractor personal information including data such as name, address, gender, disability, Social Security Number (SSN), salary, etc.;
- Employee skills, education, and certificates;
- Personal Action Processing and awards that managers can manage;
- Manager and HR workflow approvals and Budget Office position management controls
- FAIR Act for OMB Reporting;
- Separation employee clearance;
- Position-related actions that HR Specialists can approve and initiate; and

- Payroll documents and benefits that HR Specialists can manage.

There is a payroll interface that transmits PARs, Payroll Documents, and Position information to NFC. NFC uses the PAR requests to process payroll. Once customers implement HRConnect, they are able to retire legacy systems as well as automate and streamline many aspects of their HR functions. HRConnect facilitates increased efficiency and overall productivity for its customers. HRConnect Core is based on the PeopleSoft application.

The HRConnect, a FISMA High system, has full disaster recovery capabilities and implements continuous monitoring for FISMA compliance. System health and the availability are monitored by Oracle Enterprise Manager (OEM). The monitoring tool sends alerts before issues arise. The Technical Architecture team also monitors the system using cronjobs to alert on various issues. The Security team uses Splunk for event aggregation and monitoring, and other tools as listed below to check all layers of the system.

The Security monitoring tools include:

- Nessus – vulnerability scanner (scans any system with an Internet Protocol (IP) address and can recognize multiple systems) to detect vulnerabilities at the operating system and IP layer;
- DBprotect – vulnerability scanner for databases;
- WebInspect – vulnerability scanner for web applications and web interfaces;
- Splunk – collects logs from multiple types of IT systems for correlation and monitoring system activities with alerts; also used for log retention;
- Microsoft Defender – Anti-Virus

Integrated Talent Management (ITM)

ITM is Enterprise Apps's integrated talent management platform. The ITM is a Treasury branded version of the SAP SuccessFactors Human Capital Management (HCM) suite and is provided by the SAP federal services subsidiary – SAP National Security Services (SAP NS2). ITM system provides Treasury with an enterprise-wide Software as a Service (SaaS) solution that supports non-core HR business functions. This includes learning management, competency and Individual Development Plan (IDP) management, performance management, compensation management, succession planning, and workforce planning/analytics.

The purpose of the ITM/SAP NS2 system is to provide employees, supervisors, and human resources and training departments with more efficient means to manage every aspect of the human resource management functions by leveraging the COTS SAP SuccessFactors Human Capital Management (HCM) as the main component of the SAP NS2 SF HCM - Gov. The SAP NS2 SF HCM - Gov is exclusively delivered as a SaaS Cloud Service Provider (CSP) offering. The function of the system is to provide the leading SaaS offering for HCM, that conforms to the stringent guidelines and requirements established under the FedRAMP.

SAP NS2 SF HCM - Gov delivers business results by driving business alignment, optimizing people performance and building a competitive advantage through people. SuccessFactors delivers a comprehensive suite of solutions that improves executive insight and decision-making while ensuring the right people with the right skills are doing the right work.

The system infrastructure is hosted on the Amazon Web Services (AWS) GovCloud IaaS. The ITM and its data are one of many tenants hosted in this environment and is logically separated so

that it does not connect with other tenant systems. The system platform consists of virtual machines (VMs), and AWS Services logically separated into Virtual Private Clouds distributed in separate Availability Zones (AZs).

The SAP NS2 SF HCM - Gov system boundary contains the Secure Node Shared Management Services (SNSMS). Cloud Manager and Shared Services are contained in the SNSMS and shared between two boundaries (DOD and GOV). Regardless of the boundary, all systems are built and distributed utilizing scripted automation code to ensure technical consistency and compliance consistency across all logical systems.

Data integration between ITM and HRConnect further ensures accuracy and efficiency by removing the need for manual entry of data into the system for HRConnect customers.

Personally Identifiable Information (PII) for Treasury employees regarding their identity and other information described in the Interconnection Security Agreements (ISAs) is established between ITM and the HRConnect and EDM programs. Below is a quick summary of the current integrations:

- **ITM Core Data Feed:** An import of Treasury organizational and user date from HRC into the ITM. Additionally, this process provides account creation, modification and reconciliation actions.
- **Control-M Business Intelligence DataMart Feed from SAP NS2 to EDM:** Transfers DataMart files containing Learning Management, Organizational and User data from ITM to the EDM border server for IRS, OCC, and Treasury.
- **ITM to HRC Performance Ratings Feed:** A scheduled report from ITM which consolidates and transforms daily performance ratings into a single XML file for HRC consumption.
- **Monthly Workforce Analytics Import:** A monthly extract of workforce data from EDM which is imported into the ITM Workforce Analytics and Planning data cube.
- **Enterprise Human Resource Integration (EHRI) to OPM:** A monthly export of ITM Learning data delivered to OPM to meet EHRI reporting requirements. This integration is pending additional work from the SAP NS2 Operations team.

Monitoring integrations mentioned above are the shared responsibility of TMS, and resolution of issues is accomplished with the support and partnership of the accompanying programs.

SAP NS2 has developed and maintained an Information System Contingency Plan (ISCP) and an Incident Response Plan for the SAP NS2 SuccessFactors HCM Suite. These plans are located on the FedRAMP site and describe the steps to take in the event of an unexpected disruption or a security-related anomaly. Both 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.

In the event of an incident, SAP NS2 will execute a three-phase approach to recover and reconstitute the Secure Note with the SuccessFactors Suite:

- **Activation and Notification Phase**: Activation of the ISCP occurs after a disruption, outage, or disaster.
- **Recovery Phase:** The Recovery phase details the activities and procedures for recovery of the affected system. This phase includes notification and awareness escalation procedures for communication of recovery status to system stakeholders.
- **Reconstitution:** The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location.

Additional details on SAP NS2 back-up system components are in the table 2 below:

System/Component	Description
Software Used	Multiple – storage of backups is in AWS GovCloud S3 using snapshots
Hardware Used	N/A – leveraging AWS GovCloud FedRAMP High P-ATO, DoD FedRAMP+ PA
Frequency	Daily, weekly, and monthly
Backup Type	S3 snapshot for application
Retention Period	six months for the system backups

Table 2: Back-Up System Components

In Figure 3 below, are the different areas of linkage between the Enterprise Apps HRLOB and ITM.

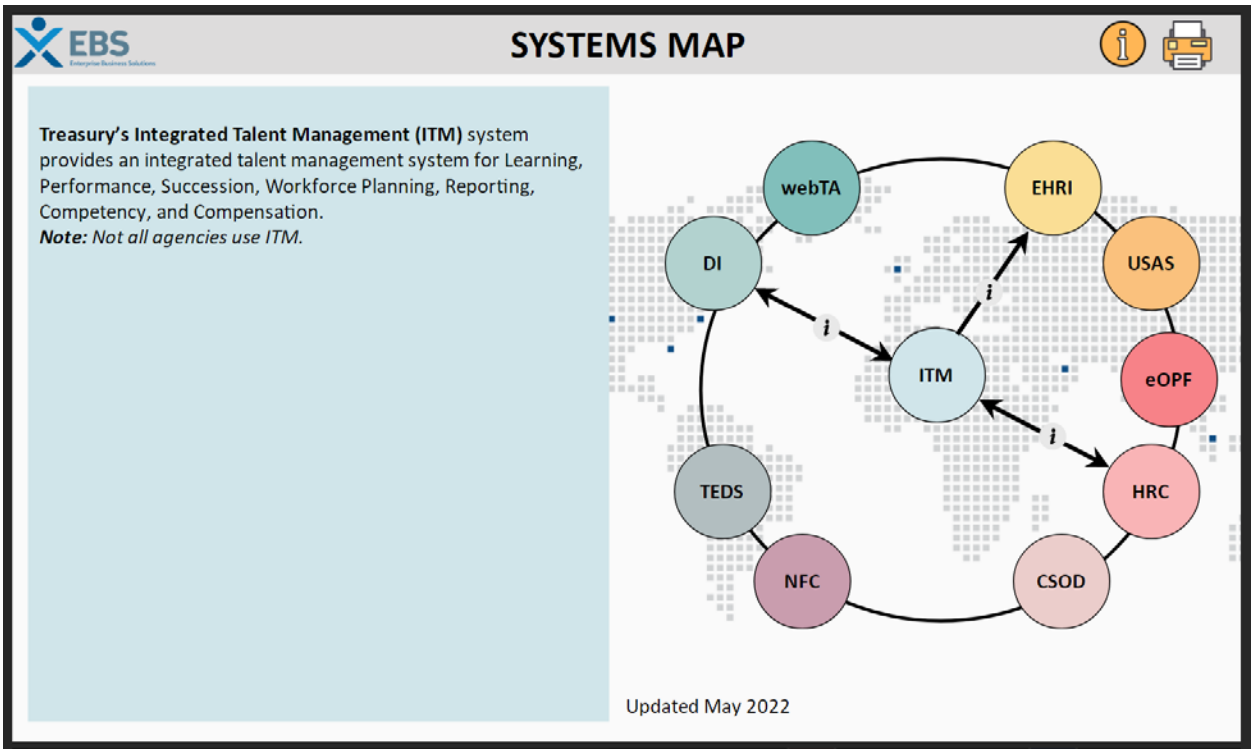


Figure 3: Connect-2-Learn ITM to/From HRC: per Systems Map

Complementary Subservice Organization Controls (CSOCs)

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

Oracle Cloud Infrastructure's Infrastructure as a Service (OCI IaaS) High GovCloud Cloud Service Provider (CSP).

The OCI IaaS CSP is the primary data center for production and non-production services for HRConnect PaaS and SaaS. The OCI IaaS CSP includes communication, utility and management servers, network cabling, routers, switches, and other communications equipment required to support network connectivity.

National Finance Center (NFC)

HRConnect features a daily bi-directional interface transmitting personnel, position, and certain payroll information to the NFC, Treasury's payroll provider. The reverse interface provides all

applied actions and NFC-generated automatic actions (annual pay increases, within-grade increases, etc.) back to HRConnect.

#	Complementary Subservice Organization Control	Related Control Objective
	OCI IaaS CSP	
1	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
	NFC	
2	Responsible for assuring that access to computer resources (data, programs, equipment, and facilities) is reasonable based on job responsibilities and segregation of duties principles and restricted to authorized individuals, processes, and devices.	CO 10
3	Responsible for assuring that only valid payroll/personnel transactions are accepted, processed completely and accurately, and reported to customer agencies.	CO 10
4	Responsible for assuring that master data is complete, accurate, and valid.	CO 10
5	Responsible for assuring user-entity requested application changes: authorized user entities complete the Form AD-3003, Software Change Request, and submits the request to the GESD mailbox for processing.	CO 10
6	When required, user entities review and approve the Functional Requirements Document (FRD) and cost estimate for the application change.	CO 10
7	When required, user entities participate in User Acceptance Testing (UAT) for application changes	CO 10

Complementary User Entity Controls (CUEC)

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

its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

Control Objective 4: Access to Computerized Applications

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

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

Control Objective 9: Secure Interface Processes

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

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

Control Objective 10: Subservice Organizations

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

1. SINQ errors, HCUP Status, and mismatch cases are corrected to ensure transactions are processed.
2. Establish controls to provide reasonable assurance that data sent and received within the HRConnect system is applicable and accurate. Authorized user entities complete the Form AD-3003, Software Change Request, and submits the request to the GESD mailbox for processing when a NFC software change is applicable.

Control Objectives and Related Controls

Enterprise Apps 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 that are presented in Section IV and are an integral component of HRConnect's description of its Enterprise Human Resources System.

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

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at Enterprise Apps.

Our examination was limited to the control objectives and related controls specified by Enterprise Apps in Section III of the report and did not extend to controls in effect at user entities.

Each user entity and its independent auditor are responsible for evaluating this information in conjunction with the internal control over financial reporting at the user entity in order to assess total internal control. If a user entity's internal control is not effective, Enterprise Apps's controls may not compensate for such weaknesses.

Enterprise Apps's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by Enterprise Apps. In planning the nature, timing and extent of our testing of the controls to achieve the control objectives specified by Enterprise Apps, we considered aspects of Enterprise Apps's control environment, risk assessment process, monitoring activities, and information and communications.

During our 2022 examination, we identified deficiencies in the Enterprise Apps's controls that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant Enterprise Apps's management's attention. We have communicated these matters to Enterprise Apps's management and, where appropriate, have reported on them separately.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance or existence of a control
Inspection	Inspection of documents and reports indicating performance of the control

In addition, as required by paragraph .35 of AT-C section 205, Assertion Based Examination Engagements (American Institute of Certified Public Accountants (AICPA), Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Objective 1: System Security Plan

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

Description of Controls

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

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

Enterprise Apps has supplemented the Department level controls by implementing specific procedures and controls at the HRConnect applications. Enterprise Apps follows and documented Treasury Directive (TD) P 85-01, and TD P 15-17, Treasury Shared Services Enterprise Cybersecurity (TSSEC), Enterprise Apps, and HRConnect specific security policies that have been made available to affected personnel, including HRConnect employees and contractors. These policies include system and application rules and expected user behaviors.

The HRConnect SSP provides an overview of the security requirements as it applies to HRConnect, and it describes the controls in place for meeting those requirements. The HRConnect SSP delineates responsibilities and expected behavior of all individuals who access the system. The Enterprise Apps Enterprise Applications Cybersecurity (EAC) for HRLoB systems (including HRConnect) maintains the HRConnect SSPs and is housed within the TFIMS.

Enterprise Apps applied RMF to HRConnect, which included conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. Enterprise Apps uses TFIMS to document this process.

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

POA&Ms to determine whether to Authorize to Operate (ATO) for HRConnect. Enterprise Apps maintains and updates SA&A documentation at least annually.

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

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

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
1.1	Enterprise Apps has documented an application-specific security plan for HRConnect System.	Inquired of Enterprise Apps personnel to determine the process of updating system security plans. Inspected policies and procedures associated with the HRConnect system to determine whether it provides an overview of security requirements. Inspected the latest HRConnect system security plan to determine whether the plan is updated periodically in accordance with their policy and procedures.	No exceptions noted.
1.2	An independent party performs on-going assessments at least annually to determine the extent to which the system's security controls are implemented and operating effectively.	Inquired of Enterprise Apps personnel to determine the process of conducting on-going control assessments. Inspected policies and procedures associated with conducting on-going control assessments to determine the frequency of the	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
		assessment and the third-party assessor involved in the process. Inspected the most recent security controls assessment performed by the independent assessor to determine whether controls were assessed on a continual basis in accordance with the policy.	
1.3	Authorizing official (AO) inspects the SSP, SAR, SRCM, and POA&Ms to determine whether to Authorize to Operate (ATO) for HRConnect.	Inquired with Enterprise Apps to determine the Security Assessment and Authorization (SA&A) process. Inspected policies and procedures to determine whether the SA&A process is formally documented. Inspected the HRConnect system ATO package to determine whether the system is authorized to operate in the production environment.	No exceptions noted.

Control Objective 2: Security Related Personnel Policies

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

Description of Controls

On-Boarding and Off Boarding

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

All Treasury Enterprise Apps employees and users with access to Sensitive But Unclassified Information (SBU) data are restricted to those who have been cleared for an interim clearance and those who have completed and favorably adjudicated background investigations. All approved users who require elevated privileges must complete the Treasury Shared Services Center security access request forms, comply with all HRConnect Rules of Behavior and related requirements. Federal employees and contractors/subcontractors are required to have a completed and favorably adjudicated background investigation that is, at a minimum, compliant with Homeland Security Presidential Directive-12 ((HSPD-12) requirements. The HSPD-12 minimum investigation is a

National Agency Check with Inquiries (NACI) or such higher-level investigation may be required by the risk level or sensitivity of the position. Individuals lacking Personnel Security approval, regardless of permission levels, will be denied access.

Employee exit procedures, including a Provisioning for Personnel (P4P) form, are completed to ensure Treasury assets are properly deprovisioned and returned. Enterprise Apps receives PIV cards of terminated employees and deactivates their physical access privileges.

Contractor exit procedures start with a P4P form being completed by the Contracting Officer's Representative (COR). Access Control reaches out to the Contractor to coordinate the return of the equipment. Once the equipment is returned, the COR is notified. For the PIV card, the Contractor mails it to the address located on the back of the card.

Training

Enterprise Apps personnel are provided with and required to take IT Cybersecurity Awareness training, Ethics training, and Privacy Awareness training on an annual basis. Enterprise Apps offers application specific training to HRConnect customers via Connect-2-Learn. Treasury employees and contractors are required to complete and sign a Rules of Behavior and confidentiality agreements prior to obtaining access to the Treasury network. New employees are required to complete the Cyber Security Awareness training and acknowledge the Departmental Offices Rules of Behavior agreement prior to obtaining access to the Treasury network. Security-related subject matters are regularly emailed to personnel and posted to the internal share drive. Enterprise Apps staff with security-related roles are required to take 4 or 8 hours of security Role-Based Training (RBT) annually.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
2.1	All Treasury Enterprise Apps employees and users with access to Sensitive But Unclassified Information (SBU) data are restricted to those who have completed and favorably adjudicated background investigations	Inquired with Enterprise Apps to determine whether the process of background investigations required for all employees and contractors who have access to SBU data. Inspected policies and procedures to determine whether all employees and users with access to SBU data are in compliance with NIST SP 800-53 Rev 4 Personnel Security. Inspected a sample of employees and contractors who have access to SBU data to verify whether they have	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
		successfully completed the Treasury Shared Services Center Security Access Request Form and have completed favorable adjudicated background investigations that are compliant with Homeland Security Presidential Directive-12 (HSPD-12).	
2.2	All Enterprise Apps personnel are required to take IT Cybersecurity Awareness training, Ethics training, and Privacy Awareness training on an annual basis.	Inquired with Enterprise Apps to determine whether there are changes or updates in the process for implementing security awareness program that includes computer-based Cyber Awareness Challenge training. Inspected security and privacy training policies and procedures to determine whether there are formal processes in place to document, track, and monitor all Enterprise Apps employee and contractors' training results. Inspected tracking records to determine whether training was monitored for staff with system access. Inspected a sample of existing users to determine whether security awareness training was completed at least on an annual basis.	No exceptions noted.
2.3	As part of the employee off boarding process, a Provisioning for Personnel (P4P) Exit Request is submitted to properly deprovision government equipment and revoke privileged accounts in the active directory and the return of property. Enterprise Apps executes the P4P. Access Control manages the return of the equipment. For Personal Identity Verification (PIV) cards, those are mailed	Inquired with Enterprise Apps personnel to determine whether the off boarding process for both Enterprise Apps employees and contractors is in place. Inspected employee exit procedures to determine whether Enterprise Apps	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
	by the Employee or Contractor directly to the Officer of Security Programs.	established and formalized the employee off boarding process. Inspected a sample of terminated employees who had accesses to the HRConnect system to determine whether P4P forms were completed, and their PIV cards were deactivated.	

Control Objective 3: Access to Facilities

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

Description of Controls

Enterprise Apps Location

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

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

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

PIV Cards

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

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

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

Oracle OCI IaaS High GovCloud CSP Location

As a Cloud Service Provider under FedRAMP authorization, EAC is not allowed to perform inspections / site visits of CSP sites. However, Enterprise Apps performed an Agency ATO of the OCI IaaS High prior to HRC's Go Live on the platform; reviewing the entire OCI IaaS SA&A package and providing an ATO statement to FedRAMP PMO. HRConnect verified Oracle CSP OCI's FedRAMP compliance prior to the HRConnect ATO, which included validation of the Physical and Environmental controls of the hosting OCI IaaS platform.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
3.1	Enterprise Apps's physical location has a security guard located within the lobby of the building requiring the signature of guest and escort by an Enterprise Apps employee. The guest's signature is maintained in a hard copy logbook at the guard station.	Inquired about the security guard in the lobby of the building and where the guest logbook is maintained. Inquired whether the logbook contains guest signatures.	No exceptions noted.
3.2	Access to Enterprise Apps's physical location is controlled using PIV cards to the elevators and floors. Access cards control access to facilities, as well as the physical access of computer equipment.	Inquired with Enterprise Apps personnel to determine whether the process for granting the appropriate security level for PIV access is in place.	No exceptions noted.
3.3	Each employee and contractor have an issued PIV card after the appropriate security approval.	Inquired with Enterprise Apps personnel to determine whether the different levels of access and the approval process are in place. Inspected a sample of employees and inspect supporting documentation to determine whether each employee and contractor was issued a PIV card with appropriate security level.	No exceptions noted.

Control Objective 4: Access to Computerized Applications

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

Description of Controls

Enterprise Apps HRConnect system stores PII data and the data is encrypted at rest and in transit. Access to HRConnect system is restricted to users with a valid PIV card, and Single-Sign-On (SSO) for internal to Treasury DO users. Certain federal Customers are passed SSO access via a Treasury TEICAM Federated TEICAM (Treasury Enterprise Identity Credential and Access Management) access for PIV SSO. Only a small quantity of identified end users are still allowed to logon via User-ID identification and password. Non-privileged users gain access to HRConnect through on-line account registration by entering a combination of their email address, the last four digits of their social security number, their last name, and a pin number that they create themselves upon registration. This process allows the user to then create a unique password that must be 12 characters long and must include at least one upper case and one lower case letter, one number and one special character. Users with access to PII are required to complete the 'TSSC Security Access Request' form, which includes signing a Privileged user Rules of Behavior. Formerly customer UAT testers were required to sign the HRConnect Program Office (HRCPO) Agreement to Safeguard Sensitive Data, but that was replaced by 'TSSC Security Access Request' form in FY21.

For PIV Card users, HRConnect passwords are not used, so they do not expire; PIV PINs changes are inherited from the Treasury PIV; outside HRConnect boundary. All passwords expire every 120 days and users are required to use the UserID or Password link to reset their password and facilitated via the Password Management System (PWMS). Users are also required to use the Forgot Password link after 3 failed login attempts. The Forgot Password link is located on the HRConnect login page. This process is the same as the account registration process that requires the user to enter a combination of their email address, last four digits of their social security number, their last name, and a custom pin number.

Access to HRConnect is dependent on the level of access needed. Non-privileged level access is granted dynamically upon account registration. This includes Employee, Contingent Worker, and Manager basic level access. All managers get access to initiate actions. Managers can assign proxies to initiate, approve, or initiate and approve actions on their behalf. Access privileges are granted based on the level of access required to support the process (e.g. for HR - processor, specialist). Privileged user accounts in production are controlled by strong passwords. Accounts are locked after inactivity. Privileged roles that are no longer needed are manually removed by Customer Service.

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

* Super User access, which grants users access to all panels and agencies in HRConnect.

* Privileged level access to HRConnect, which includes any roles not available to the agency via Bureau Maintenance User Access Maintenance. Examples of these roles include, but are not limited to, HR Super role and TR Bureau Super role.

The Treasury Shared Service Center Security Access Request form is signed by the user, the user's manager, and the agency representative. The approved form is then sent to Customer Service via Treasury Service Desk ticketing system or emailed to the Customer Service Team E-mail box. A ticket is created for setup. Customer Service grants the access and notifies the user of the UserID and temporary password. Customer Service then notifies the agency that the access has been granted and the user has been provided with their credentials. User accounts are deactivated via the Personnel Action Request (PARs) process for terminating users. User IDs that have been deactivated due to termination are automatically locked. An automated process runs every night. First, it scans all the PARs for any users that are contingent workers or employees that are no longer active as of that day or prior. The process then updates those user profiles as follows: locks the account, removes the primary permission list, and removes all the roles. This prevents the account from accidentally being unlocked and being usable.

Customer Service performs additional audits on user accounts. Privileged and Superuser accounts are analyzed by Customer Service quarterly to determine which accounts and roles are no longer needed due to termination or transfer. Health check reports are generated weekly. The health check consists of several reports that are reviewed by Customer Service. Customer Service reviews the health check report to identify user accounts with duplicate IDs. The health check review includes a review of the PAR Approving Officials table for both Terminated users and name changes. The following two reports are sent to the agencies to review: Positions that are encumbered by more than one employee, Active employees reporting to inactive positions to review and take the necessary action.

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

* Border Server

- Customer Service collects the forms, ensures they are complete, and then forwards the form to the Technical Architecture team for set up. The Technical Architecture team communicates the userID and Password to the user. Once the account is set up, Customer Service notifies the agency that the account set up is complete.

* TOAD Access

- Tool for Oracle Application Developers: Toad is a database management toolset from Quest Software for managing relational and non-relational databases using SQL aimed at database developers, database administrators, and data analysts.
- Customer Service collects the forms, ensures they are complete, and then forwards the form to the DBA team for set up. The DBAs communicate the userID and Password to the user. Once the account is set up, Customer Solutions notifies the requester that the account set up is complete.

* ITM Privileged and Non-Privileged Access

Enterprise Apps's Customer Service Team collects the forms for elevated access, ensures they are complete, and then forwards the form to the team for setting up. Access is restricted to users with a valid logon identification and pin. Once the account is set up, Customer Service notifies both the user (with the credentials) and the agency that the account set up is complete. Password reset requests are facilitated through automated email notification. Daily reports are provided to all users who have accessed the system within a specified number of days. Admin accounts are manually reconciled intermittently; non-admin accounts are inserted/reconciled by the HRConnect Data Feed.

Complementary User Entity Controls

User entity auditors should determine whether user entities have established controls to provide reasonable assurance to properly grant access to the systems to users who have been vetted by their organization's security requirements. Additionally, reasonable assurance to properly provide appropriate levels of privileged user access to the systems to users who have a bona fide need and have met their organization's security requirements. Finally, user entity auditors must determine whether user entities have established controls to provide reasonable assurance to properly assign security roles to users based on their role in the system (e.g. personnel specialists would hold the HR Specialist role vs. a manager who would hold the manager role in HRConnect).

Remote Access

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

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
4.1	Each employee with access to PII has been granted access and completed the HRConnect Program Office (HRCPO) Agreement to Safeguard Sensitive Data.	Inquired with Enterprise Apps personnel to determine whether the process for granting access to HRConnect system and the PII environment is in place. Inspected the access provisioning procedure to determine whether the process of granting system accesses is in place. For sampled new system users, we obtained and inspected TSSC Security Forms to determine whether TSSC Security Forms are completed.	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
4.2	All passwords expire every 120 days and users are required to use the UserID or Password link to reset their password and facilitated via the Password Management System (PWMS). Users are also required to use the Forgot Password link after 3 failed login attempts.	Inquired with Enterprise Apps management to determine whether the password configuration setting for HRConnect system is in place. Inspected a screenshot of system configuration setting to determine whether the password is automatically set to expire every 120 days and user accounts are locked after three (3) failed login attempts.	No exceptions noted.
4.3	Privileged accesses that are no longer needed are manually removed by the Customer Service.	Inquired with Enterprise Apps management to determine whether the process for manually removing privileged accesses from HRConnect system is in place. Inspected a list of Enterprise Apps separated employees and current active privilege accesses within HRConnect system and the database system to determine whether privileged access was properly removed.	No exceptions noted.
4.4	Privileged user access (including more advanced and Super-level) can only be provisioned by the Enterprise Apps Customer Service team and requires a Signed Treasury Shared Service Center Security Access Request form to be completed.	Inquired with Enterprise Apps management to determine whether the process for granting and removing privileged user accesses and approving the access of generic Database Administrators (DBA) accounts is in place. Inspected policies and procedures associated with privileged access management to determine whether privileged and Super Users access requirements are defined. Inspected a sample of privileged users Security Access Request Forms to determine whether the proper approval was completed, and access had been granted accordingly.	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
4.5	The Treasury Shared Service Center Security Access form is used to grant access to the following applications that are included in this audit review: -Border Server -Toad Access	Inquired with Enterprise Apps management to determine whether the process for granting Border Server, Toad Access, and Remote Access is in place. Inspected one user's Border Server form to determine whether the form was completed, and the form was forwarded to the Customer Service team for account set up. Inspected one user's Toad Access form to determine whether the form was completed and forwarded to the DBA team for set up.	No exceptions noted.
4.6	User accounts are deactivated, automatically locked, and removed for terminated users.	Inquired with Enterprise Apps management personnel to determine whether the process of managing terminated user accounts in place. Inspected procedures associated with the user access termination process to verify whether terminated users' system accounts are deactivated, locked, and removed from the system. For both separated users, determined whether access was properly removed.	No exceptions noted.
4.7	Privileged users are reviewed by Customer Service quarterly.	Inquired with Enterprise Apps management to determine whether the process of reviewing privileged users is in place. Inspected policies and procedures regarding periodic review of users accounts. Inspected latest quarterly review of privileged user accounts conducted by the Customer Solutions to determine whether the review was documented as required.	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
4.8	Health check reports are generated weekly and reviewed by Customer Service.	Inquired with Enterprise Apps management to determine whether the process of reviewing the health check reports is in place. Inspected policies and procedures associated with the process of periodic reviews of health check reports to determine whether the review frequency process is in place. Inspected evidence of health check reports to determine whether Customer Service generated and reviewed the reports.	No exceptions noted.

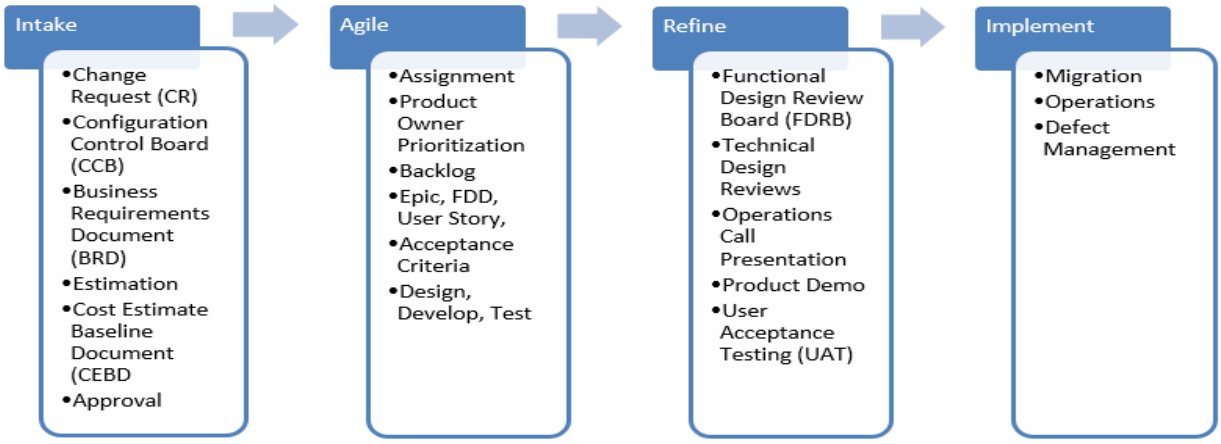
Control Objective 5: Software Development and Maintenance Activities

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

Description of Controls

Enterprise Apps has documented the configuration management process for HRConnect applications that includes roles, responsibilities, reviews, and approvals of configuration changes. The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the intake through implementation.

Our process is defined in four (4) different categories: Intake, Agile, Refine, and Implement.



Intake:

Proposed change requests (CRs) or new ideas are submitted by customer representatives or internal team members to the Enterprise Apps Intake Team. The Enterprise Apps Intake Team utilizes the request management module in ServiceNow to manage all incoming requests. This ServiceNow module allows the team to manage the Enterprise Apps Intake process from initial request through turnover to the HRConnect Product Team. Proposed CRs are reviewed weekly by a team of program representatives including functional analysts, developers, project managers and program management. During that meeting leadership makes decisions about whether or not to approve the proposed CR to move forward in the process.

The HRConnect Team conducts a monthly Configuration Control Board (CCB) meeting with customer agency/bureau representatives and internal stakeholders, including Enterprise

Applications Cybersecurity. During the CCB meeting, the Change Requests are reviewed and feedback is requested from the customers. The HRConnect team records the CCB minutes and distributes them to the participants. If the CR is recommended/selected, alternative impacts, both positive and negative, are documented if appropriate.

If the CR is approved to move forward, a determination is made whether a Business Requirements Document (BRD) should be drafted or if a BRD waiver is appropriate. BRD Waivers track program management approval to bypass the BRD documentation requirement. The waiver must contain justification for not preparing a BRD and be approved and signed by management (i.e. regulatory, mandatory, low impact, etc.). If a BRD is required for a CR, the team drafts the BRD and obtains approval signatures.

The CR is assigned to an Agile Team for estimation. A cost estimate is completed for the CR based on the BRD and reviewed with program leadership. Program leadership makes a determination if the cost estimate qualifies to be presented to executive leadership during the weekly Project and Portfolio Management (PPM) meeting. If the CR cost estimate is under $10,000 and/or it is in internal facing project with low visibility, a PPM waiver is completed. The PPM waiver tracks program management approval to bypass the PPM meeting requirement. The waiver must contain justification and approval signature. Items reviewed at the PPM meeting require an Idea Document, which provides the background of the request and the cost estimate. The Idea Document is presented to executive leadership for approval.

Upon executive approval, Enterprise Apps Intake schedules a conference call with the customer to review the cost estimate. Following that meeting, a Cost Estimating Baseline Document (CEBD) is created. The CEBD summarizes project scope, roles and responsibilities, assumptions, and costs. The CEBD is forwarded to the customer for review and approval signature. Once the customer signs the CEBD and returns it to the Enterprise Apps Intake team, the funding collection process begins (if applicable). Funds are often exchanged via the Inter-Agency Agreement (IAA) modification process. After the IAA modification is developed and executed by both parties and any necessary contracting actions have been completed, the Enterprise Apps Intake Team hands off the project to an HRConnect Agile Team to execute the work.

Agile:

The Agile Process is a multistep collaborative process that begins with supporting the intake process with estimation and resumes after official project handoff from the Enterprise Apps Intake team. Upon project turnover, the CR is added to the Agile Team's backlog and the Product Owner prioritizes the work. Analysis, design, development, testing, product demos are completed in Sprints and implemented after customers validate changes during a user acceptance test (UAT) period.

Enterprise Apps uses ClearQuest change management software to control changes for HRConnect and maintain application baselines throughout the process. The change management software manages the approvals, audit trails, coding, testing, and publication of the software changes. The software allows automated workflows and email notifications to ensure that appropriate team members are alerted in near real-time when action is required; and software changes, along with associated requirements, are documented. Change requests are tested according to development organization guidelines and approved prior to implementation.

Refinement

An Epic User Story Functional Design Document (EUSFDD) is drafted and reviewed internally in the Functional Design Review Board (FDRB) meeting with representatives from the Functional, Development, Quality Assurance, Customer Service, and Enterprise Applications Cybersecurity Teams in attendance. Adjustments are incorporated into the document based on internal team feedback. Enterprise Applications Cybersecurity Team provides Security Impact Assessments (SIA) of the CRs identifying risk, security controls impacted and cybersecurity actions. The EUSFDD is ultimately approved by the Director of HRConnect Products Management Team

An Enterprise Apps Developer performs a Technical Design Document (TDD) review to walk through the changes and impact based on the EUSFDD. The TDD is a working document and is completed at the end of development. Minutes from the technical review session are included in the technical data package for the CR stored in the change management repository.

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.), an EUSFDD and/or TDD may not be required. A waiver is completed and submitted for approval by the designated Federal Manager.

The development and technical documentation are considered complete, when the CR includes:

- an EUSFDD or EUSFDD waiver,
- a TDD waiver, and;
- Technical peer review performed as described in the Software Peer Review Check List.

The Agile Teams present and share CR changes with the customers with product demonstrations and presentations.

Implementation:

Once approvals are received, the change is migrated to the production environment by an independent partner.

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

Customer cybersecurity points of contact are invited to come onsite (virtually) and review the HRConnect SA&A package documentation, typically annually, which often includes information on recent and upcoming major changes to the system.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
5.1	Enterprise Apps has documented the configuration management procedures for HRConnect. The procedure document defines: • Roles and responsibilities • Requirements for the review and approval of configuration changes.	Inquired with Enterprise Apps personnel to determine whether Enterprise Apps has documented the formal configuration management process for HRConnect applications including the frequency of the management review of the procedures document. Inspected policies and procedures for the configuration management process. The documented whether the process included: • Roles, responsibilities, procedures, and documentation requirements for configuration management and systematic policy implementation. • Requirements for the regular review and approval of configuration changes. Inspected a sample of 9 closed change requests and 7 active change requests to determine whether Enterprise Apps consistently implemented policies and procedures.	No exceptions noted.
5.2	All changes to the HRConnect system are authorized, documented, tested, and approved.	Inquired with Enterprise Apps personnel to determine whether the change management process including documentation, approval requirements, and the establishment of the Change Control Board (CCB) is in place. Inspected procedures associated with change management process to determine whether the existing change management process from initiation to approval and a list of CCB members who are responsible for reviewing of all program changes prior to	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
		implementation and policies and procedures associated with configuration management is in place. Inspected 9 closed and 7 active change requests to determine whether all changes were authorized, documented, tested, and approved.	
5.3	For approved change requests, determinations are made whether a Business Requirements Documents (BRD) or BRD waiver forms are needed. BRD Waivers track program management approval to bypass the BRD documentation requirement. The waiver must contain justification for not preparing a BRD and be approved and signed by management. If a BRD is required for a change request, the team drafts the BRD and obtains approval signatures.	Inquired with Enterprise Apps personnel to determine whether the process BRD or a BRD waiver form is required to be created when a change request is approved. Observed the BRD/BRD waiver process to determine whether the process is implemented. Inspected 9 closed and 7 active change requests to determine whether Enterprise Apps documented and maintained all correspondent approved BRD or BRD waiver forms.	No exceptions noted.
5.4	Cost estimates are completed for Change Requests based on the associated BRD and are reviewed with program leadership to make a determination if the cost estimate qualifies to be presented to executive leadership during the weekly Project and Portfolio Management (PPM) meeting.	Inquired with Enterprise Apps personnel to understand the process of completing the cost estimates for change requests and the approval process. Inspected procedures to determine whether the process for completing cost estimates for change requests is documented and approved. Inspected 9 closed and 7 active change requests to determine whether cost estimates were drafted and agreed upon. If cost estimate was not agreed upon, verified sampled tickets have valid Project and Portfolio Management waivers.	No exceptions noted.
5.5	An Epic User Story Functional Design Document (EUSFDD) is drafted, reviewed, and approved. In addition,	Inquired with Enterprise Apps personnel about the EUSFDD to determine whether the review and	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
	Enterprise Apps developers perform Technical Design Document (TDD) reviews to walk through the changes and impact based on the EUSFDD.	approval process during the refinement phase is in place. Inspected the EUSFDD template to determine whether the review and approval process is fully documented. Inspected the 9 closed and 7 active change requests to determine whether EUSFDD reviews and approvals were completed.	
5.6	Once approvals are received, the change is migrated to the production environment by an independent partner.	Inquired with Enterprise Apps personnel to determine how changes are migrated into production. Inspected policies and procedures to determine how changes are migrated to the production environment after appropriate approvals. Inspected the closed change requests to determine whether all changes were migrated into production by an independent partner.	No exceptions noted.

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

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

Description of Controls

For HRConnect on OCI CSP, Annual Manual security inspection, and monthly automated security vulnerability and security configuration scans are performed on all Enterprise Apps Cisco firewalls. Enterprise Apps CyberSecurity inspects the security of the HRConnect firewalls and delivers reports semi-annually and upon changes. On behalf of a System Owner, ISSO, and ISSM, Enterprise Apps CyberSecurity security engineers conduct a monthly vulnerability assessment, and system security configuration scans to identify network vulnerabilities. For HRConnect on OCI CSP, the vulnerability and configuration scans are run nightly. Enterprise Apps analyzes the identified vulnerabilities and either mitigates the vulnerability or documents it is required for production processes. Enterprise Apps scans the various layers of HRConnect based on Treasury policy and Enterprise Apps CyberSecurity team formal SOP. Vulnerabilities are provided to

System Owners and Technical staff for remediation. For HRConnect on OCI CSP, monthly scans are tracked in security scan software's dashboard reports. Findings are tracked for remediation, and vulnerabilities identified from monthly scans are added as POA&Ms based on policy's remediation schedule.

Enterprise Apps's vulnerability management process follows Departmental policy on Flaw Remediation including patch management and System Updates to ensure system flaws are identified, reported, and corrected. Patches are prioritized and approved through Enterprise Apps and are tested on non-production systems prior to migration to and installation on all production systems.

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

HRConnect collects audit logs from the various HRC layers: PeopleSoft application and supporting operating system and DBMS audit logs. These are consolidated into Splunk centralized repository where dashboards segregate and help identify potential indicators of compromise.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Operating Effectiveness Testing
6.1	For HRConnect on OCI CSP, monthly scans are tracked in security scan software's dashboard reports. Findings are tracked for remediation, and vulnerabilities identified from monthly scans are added as POA&Ms based on policy's remediation schedule.	Inquired of Enterprise Apps personnel regarding the process of conducting monthly scans to determine whether the process is being followed or if any changes have been made and documented. Inspected policies and procedures associated with conducting monthly scans. Selected a sample of findings to determine whether POA&Ms were created and tracked through resolution.	No exceptions noted.
6.2	Enterprise Apps Cybersecurity security engineers conduct a monthly vulnerability assessment and system security configuration scans to identify network vulnerabilities. For HRConnect on OCI CSP, the vulnerability and configuration scans are run on Tuesdays and Fridays. Enterprise Apps analyzes the identified vulnerabilities and either mitigates the	Inquired with Enterprise Apps personnel regarding the process for conducting vulnerability assessment and system security configuration scans to identify network vulnerabilities. Inspected policies and procedures outlining the process for conducting vulnerability assessment and system security	No Exceptions noted .

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Operating Effectiveness Testing
	vulnerability or documents it is required for production processes.	configuration scans to identify network vulnerabilities. Inspected documentation of completed monthly vulnerability assessment and system security configuration scans. Inspected the scan results to determine whether any high-risk vulnerabilities were identified. As applicable, obtained supporting documentation that evidences the remediation of identified vulnerabilities.	
6.3	Penetration testing is conducted annually to exploit vulnerabilities and insufficiently configured security controls to determine whether a user could obtain unauthorized access to Enterprise Apps's IT operational environment.	Inquired of Enterprise Apps personnel regarding the process for conducting penetration testing. Inspected procedures outlining the process for conducting penetration tests on Enterprise Apps IT operational environment. Inspected the latest penetration testing results to determine whether the testing was conducted annually.	No exceptions noted.
6.4	HRConnect collects audit logs from the various HRC layers: PeopleSoft application and supporting operating system and DBMS audit logs. These are consolidated into Splunk centralized repository where dashboards segregate and help identify potential indicators of compromise.	Inquired with Enterprise Apps personnel regarding the process of monitoring unusual activities. Inspected procedures outlining the process for monitoring unusual activities. Inspected the incident related evidence to determine whether remediation steps are taken.	No exceptions noted.

Control Objective 7: Accuracy Testing Methods

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

For each connection method, HRC uses technical methods to validate that the connection is established, and then validates that the data transfer occurs accurately.

Data Integration with External Applications

HRConnect exchanges data with business partners using three different platforms: Border Server services, SOA web services, and Enterprise MuleSoft Application Program Interface (API) services.

Border Server

Control-M runs various jobs to push and pull data between the HRConnect border server and business partner systems. With one exception, all of these interfaces are conducted using the SFTP protocol. That exception is the USDA National Finance Center (NFC). Interfaces with the NFC use the FTP protocol. Currently, the NFC only supports FTP. However, they are in the midst of moving to SFTP, which HRConnect will adopt as soon as it becomes available.

If critical Control-M interfaces jobs fail, Control-M will send an email and warning page to the on-call DBA. As is appropriate, Control-M will also automatically rerun the file transfer job several times before completely stopping.

If a critical pager notification is received, the On-Call DBA will manually inspect the Control-M Job status by reviewing the available job log output files for the cause of the error. Typically, the log will contain the cause of the failure and will be helpful for troubleshooting and issue resolution.

SOA Web Services

The purpose of SOA Web Services is to verify the connection and data transfer were accurately and correctly completed or sent and received.

1. When web services fail to send a message to a partner system, notifications (email alerts) are sent out to recipients' setup using configuration.

2. Regardless of the status of a web service message transmission (success or failure), it is logged to "Message Monitor "(a mechanism to log and retrieve messages in HRC), where support personnel can view it and take corrective action.

3. In case of discrepancies between systems, such as USAccess and HRC, there are reports generated in PDS part of HRC UI to investigate further and take corrective action.

Enterprise MuleSoft Services (EMS) Application Program Interface

Data is transmitted via near-real time API (application program interfaces) transmissions. API connections are brokered using the Treasury Enterprise Mulesoft Services (EMS) System (Treasury Mulesoft High – FIPS High Designation). Customer uses Treasury HRConnect APIs deployed in EMS MuleSoft to fetch or update data in HRConnect.

Connection description info and data elements transferred: Treasury HRConnect NewHire API is a secure Representational State Transfer Architectural Style (REST) API which allows API consumers, such as USA Staffing, to transmit New Hire on-boarding data (standard forms such as OF-306, custom forms) to HRConnect. Treasury's NewHire API transmits on-boarding data received from USA Staffing to customer's system. This data transmission eliminates time consuming manual and error-prone data entry processes in multiple systems. Automated data transmission will also further support quick background investigations, as well as Treasury's Contractor Suitability Processing Request Form for new hires.

MuleSoft platform does not store any application data so there is no data persistence – it is a transient pass-through to fetch/update data from backend systems (ex: HRConnect).

Integrated Talent Management (ITM)

The Integrated Talent Management (ITM) system receives data from HRConnect. The SaaS Ops team validates the Learning User Connector - Federal, Learning Organization Connector, and Learning User Connector-SF all run successfully in ITM each morning Monday-Friday to ensure the organizational and user data from HRConnect was successfully added to ITM Learning. In the rare instance the connector fails, NS2 is both emailed and contacted through their ticketing system. An incident is also posted on the Enterprise Apps Incident Reporting Hub. If the connector is run again on the same day, there is no lapse in information passing from HRConnect to ITM.

All ITM accounts are automatically created from HRConnect's user data, and no ITM accounts are manually created or deleted. Only Enterprise Apps can connect to the vendor server. The vendor server cannot initiate a connection to the Enterprise Apps border server. The files are encrypted with the vendor's Pretty Good Privacy (PGP) key before being transferred to the vendor. Encrypted SFTP sessions are used to transfer files. PKI is used to authenticate to the vendor server. Files are encrypted 'at rest' on the HRConnect server using Oracle storage area network (SAN) encryption technologies.

Accuracy Testing Methods:

The ITM Program acts as a custodian for customer data housed within the application and is not responsible for its accuracy or integrity; that responsibility belongs to the bureau specific administrators. This nuance applies to the data that ITM inherits via the HRConnect core data feed, and other existing integrations. In the event a data error is identified by the bureau administrators, the process for correction is also in inherited from HRConnect. It is the responsibility of the participating agency's process owner to take appropriate steps to correct the findings. Follow-up communication with customers regarding issues is via email.

The successful transmission of the data is validated by daily monitoring of the SAP NS2 SFTP, where inbound files are deposited by the Enterprise Apps border server. The absence of a file

indicates a failure of the process. To remediate the issue, the ITM program reports the issue to both HRC and SAP NS2 via tickets followed by escalation via email. Individual incidents caused by timing issues or errors processing the data, are resolved and addressed in the next overnight file. Complex issues that result in long term disruptions to the flow of data, are communicated to customers via email along with root cause analysis information and a plan of action to remedy.

ITM Change Control Board:

If a change request affects the HRConnect data feed, an in-take request is created with HRConnect to follow the HRConnect in-take processes.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
7.1	Data from HRConnect is received by the Integrated Talent Management (ITM) system. If connector fails, NS2 is both emailed and contacted through their ticketing system. An incident is also posted on the Enterprise Apps Incident Reporting Hub.	Inquired of Enterprise Apps personnel regarding the process for monitoring the control of transmission of data between ITM and HRConnect. Inspected the procedures for monitoring and control of transmission of data to determine whether specific procedures are documented related to the transferring of organizational and user data between ITM and HRConnect. Inspected an example of an incident to determine whether NS2 received notifications through email and remediated if necessary.	No exceptions noted.
7.2	Files are encrypted in transit and at rest.	Inquired of Enterprise Apps personnel to determine the process of file encryption policy, in transit and at rest. Inspected policies and procedures to determine whether the process of file encryption for HRConnect is documented. Inspected the configuration settings used for both files in transit and at rest to determine whether the requirements are met.	No exceptions noted.
7.3	All proposed changes to the ITM system are submitted as a ServiceNow ticket. A CCB meeting	Inquired with Enterprise Apps personnel regarding the ITM change request process	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
	is held monthly for customers, stakeholders, and owners to discuss system changes, potential improvements, and efficiencies regarding the requests.	(HRConnect in-take processes) including documentation and approval requirements. Inspected configuration management procedures to determine whether the ITM change request process is documented. Inspected all closed change tickets from a CCB meeting to determine whether in-take request tickets were created and went through CCB approval.	

Control Objective 8: Customer Interagency Agreements

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

Description of Controls

Enterprise Apps establishes an Interagency Agreement (IAA) with the Requesting Agency requesting services performed by Enterprise Apps's Shared Services Programs (SSP) and the Department of Treasury. The IAA

conforms to the government-wide guidance prescribed by the Bureau of the Fiscal Service (Fiscal Service) in Treasury Financial Manual, Vol. I, Part 2, Ch. 4700, App. IO, (May 2019). The IAA authorizes SSP to provide the Requesting Agency service as described in the service description(s).

Each year, Enterprise Apps works closely with its customers to agree on the scope and nature of services to be provided by Enterprise Apps. Customer responsibilities in addition to Enterprise Apps responsibilities are captured within the IAA. Enterprise Apps documents changes to the IAA using form 7600 A&B, as well as product-specific addenda.

Enterprise Apps's customers are provided the opportunity to participate in survey polls conducted by Treasury.

Enterprise Apps performs an annual HRConnect Customer Satisfaction Survey where Enterprise Apps determines the survey timeline and content for the year. The schedule for this survey is shared with the customers during the Configuration Control Board (CCB) meeting prior to the survey start date. These survey results are summarized and presented during the subsequent CCB meeting.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
8.1	Enterprise Apps has Interagency Agreements (IAA) with all non SSP Customers utilizing Enterprise Apps products and services. Customer and Enterprise Apps responsibilities are captured within the IAA. Mid-year changes to the IAA require modifications to the form 7600 A&B. SSP customers utilize an internal transfer process to exchange funds.	Inquired with Enterprise Apps personnel regarding the process for establishing IAA with non SSP customers to determine whether the process is conforming to the government-wide guidance prescribed by the Bureau of the Fiscal Service. Inspected policies and procedures associated with IAA to determine whether it captures customer and Enterprise Apps responsibilities. Inspected a sample of IAA to determine whether the IAA captured both the customer and Enterprise Apps responsibilities, as well as contained proper approval.	No exceptions noted.
8.2	Enterprise Apps performs an annual HRConnect Customer Satisfaction Survey where Enterprise Apps will determine the survey timeline and content for the year. Schedule for survey is shared with customers during the configuration control board (CCB) meeting prior to the survey start date. Survey results are summarized and presented during the subsequent CCB meeting.	Inquired with Enterprise Apps personnel regarding the HRConnect Customer Satisfaction Survey to determine the process, and timeline, and content for the year. Inspected the schedule for the survey to determine whether the date of the survey was shared with customers during the CCB meeting prior to the survey start date. Inspected a sample of survey results and CCB meeting minutes to determine whether results were discussed during the monthly CCB meetings.	No exceptions noted.

Control Objective 9: Secure Interface Processes

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

Description of Controls

Enterprise MuleSoft Services (EMS) Application Program Interface

API applications deployed in MuleSoft running on WC2-High cloud fetch/update HRConnect data using industry standard security protocol TLS V1.2 and data traversing through AWS and Treasury networks is encrypted and secured through Treasury-WC2H IPSec tunnel and Treasury-OCI IPSec tunnel. MuleSoft Wc2-High platform runs on FIPS-140-2 standard security model so data at rest and data in transit are secured and encrypted. MuleSoft platform does not store any application data so there is no data persistence – it is a transient pass-through to fetch/update data from backend systems (ex: HRConnect). All log files generated in MuleSoft by application are ingested into Splunk and are preserved for search, reporting and analytics. No PII information is captured in these logs. All passwords/keys used in MuleSoft applications are encrypted, all APIs exposed are secured using client_id/client_secret or oauth 2.0 tokens.

Data is transmitted via near-real time API (application program interfaces) transmissions. API connections are brokered using the Treasury Enterprise Mulesoft Services (EMS) System (Treasury Mulesoft High – FIPS High Designation). Partners use Treasury HRConnect APIs deployed in EMS MuleSoft to fetch or update data in HRConnect.

Connection description information and data elements transferred: Treasury HRConnect NewHire API is a secure REST API which allows API consumers, such as USA Staffing, to transmit New Hire on-boarding data (standard forms such as OF-306, custom forms) to HRConnect. Treasury's NewHire API transmits on-boarding data received from USA Staffing to HRConnect system after transforming it to conform to HRConnect schema. This data transmission eliminates time consuming manual and error-prone data entry processes in multiple systems. Automated data transmission will also further support quick background investigations for new hires.

SOA Web Services

SOA web services (a real time XML synchronous message) provides a non-persistent two-way transmission service between HRC and customers. Access between HRConnect SOA services and the customers, is facilitated by a non-persistent two-way web services connection. The HRC

Service Orient Architecture (SOA) provides connectivity to support data exchanges between these systems including the exchange of all updated information in either system. Authentication mechanism employed; authenticated certificates. Each HRConnect SOA transaction is authenticated via authenticated certificates. Once authenticated, the SOA service sends the transactions via encrypted SSL.

Border Servers

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

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

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

Interface files are encrypted in transit. Only the SFTP and Connect: Direct FTP+ protocols are allowed for file transfers.

Secured Interface

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

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

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

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

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

The Enterprise Apps TA team establishes password-based connectivity to the third-party vendor servers using SFTP and the newly provided credentials. Then the Enterprise Apps TA team provides the Treasury SSH public key to the partner and requests that they add the Treasury public key to the partner's PKI KeyStore. Once this is completed, the Enterprise Apps TA team can establish key-based authentication instead of password-based authentication. Once key-based authentication is established, the Enterprise Apps TA team automates the file transfer process. The Enterprise Apps Deployment team provides the connectivity information (Unix ID and password,

EA border server name/IP address, and UNIX directory where interface files are stored) to the User Entity's technical contact.

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

The Enterprise Apps 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 Enterprise Apps border server. The TA Work Order contains information including the names of the files being transferred, the size of the files being transferred, and the transfer schedule. The Enterprise Apps developer refers to the CQ TA Work Order in the interface program Customer Service Request (CSR) migration notes so that the Control-M updates are made at the same time as the interface program is migrated.

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

Complementary User Entity Controls

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

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
9.1	New interface requests are managed through the Enterprise Apps Intake Process. The Enterprise Apps Cybersecurity Team/ISSO reviews the change request that includes the information of data to be transmitted to or from HRConnect. When the new interface is approved, the Enterprise Apps Cybersecurity team creates an Interconnectivity Security Agreement (ISA) and/or Memorandum of Agreement (MOA) if required.	Inquired with the Enterprise Apps Cybersecurity Team regarding the Enterprise Apps HRConnect change control process for new interface requests. Inspected policy and procedures outlining the interface management process. Inspected a sample of new system interfaces to determine whether ISA/MOAs are created and approved by the Enterprise Apps Cybersecurity Team.	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
9.2	Enterprise Apps reviews and updates ISA/MOAs every three years.	Inquired of Enterprise Apps personnel regarding ISA/MOA reviews. Inspected the procedures outlining the process of reviewing and updating ISA/MOAs. Inspected the latest management review evidence to determine whether Enterprise Apps reviewed and updated the ISA/MOAs every three years.	Exception Noted. Determined that 1 out of 7 sampled ISA was not updated or reviewed within the 3-year period. ***Management Response***: An internal Plan of Action and Milestones (POA&M) was created (#47283) to track this finding. The POA&M is tracking the Interconnection Security Agreements (ISAs) requiring renewal and remediation milestones which include: (1) validating all interconnections which require ISAs in FY23 Q1, and (2) renewing all expired ISAs by no later than FY23 Q2. The long-term goal is to implement an automated solution for ISA tracking and renewal as part of our Treasury Governance, Risk, and Compliance (GRC) initiative, which is targeted for implementation in FY23.
9.3	The Enterprise Apps Deployment team provides the User Entity's technical contact with an Enterprise Apps Access Request Form if the user entity provides technical contacts to the TA team and to the third-party vendor as necessary. The user entity or third-party vendor provides IP addresses of user entity's data required to transmit the data to the Enterprise Apps border servers (both test and production Enterprise Apps border servers). The Enterprise Apps TA team then creates a Fiscal Services CR requesting the Fiscal Services update firewall rules to allow the transmission between the user entity or third-party vendor to the Enterprise Apps border servers.	Inquired with Enterprise Apps personnel to determine the process for transmitting data to Enterprise Apps border servers is in place. Inspected associated procedures surrounding the process for requesting access for transmitting data to Enterprise Apps border servers. Inspected sampled requests to determine whether the process was followed appropriately.	No exceptions noted.
9.4	Enterprise Apps TA team establishes password-based connectivity to the third-party vendor servers using SFTP and the newly provided credentials. Then the	Inquired of Enterprise Apps personnel to determine the process for establishing password-based connectivity	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
	Enterprise Apps TA team provides the Treasury SSH public key to the partner and requests that they add the Treasury public key to the partner's PKI KeyStore. Once this is completed, the Enterprise Apps TA team can establish key-based authentication instead of password-based authentication. Once key-based authentication is established, the Enterprise Apps TA team automates the file transfer process.	and providing public keys to interface partners. Inspected procedures regarding process for establishing password-based connectivity and providing public keys to interface partners. Inspected screenshots of public key to determine whether key based authentication is established for new third-party vendor servers.	
9.5	The Enterprise Apps developers are 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 Enterprise Apps border server. The TA Work Order contains information including the names of the files being transferred, the size of the files being transferred, and the transfer schedule. The Enterprise Apps 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.	Inquired with Enterprise Apps personnel regarding the process on creating work orders for Control-M and the approval process for production implementation. Inspected associated procedures surrounding the process on creating work orders for Control-M and the approval process for production implementation. Inspected a Sample of CSRs to determine whether Control-M related changes were created through TA Work Orders.	No exceptions noted.

Control Objective 10: Subservice Organizations

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

Description of Controls

Oracle OCI GovCloud Cloud Service Provider (CSP):

HRConnect resides upon the Oracle Cloud Infrastructure (OCI) Infrastructure as a Service (IaaS) GovCloud Cloud Service Provider (CSP). Treasury Enterprise Apps reviewed the FedRAMP SA&A package and issued a Treasury Agency ATO of Treasury use of the OCI IaaS High GovCloud CSP December 6, 2019. Treasury also provided a FedRAMP-based ATO of OCI IaaS High GovCloud. HRConnect (on OCI) obtained its formal Agency Authority to Operate (ATO) January 31, 2020. Oracle OCI High GovCloud received its FedRAMP ATO 4/10/2020. Treasury ended its formal sponsorship of OCI IaaS GovCloud once the FedRAMP PMO issued its PATO of OCI IaaS (see https://marketplace.fedramp.gov). EAC reviews OCI's FedRAMP Continuous Monitoring information via monthly ConMon meetings and annually via OCI IaaS SA&A package reviews when the documentation is provided by Oracle.

National Finance Center

Enterprise Apps 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 related financial reporting of HRConnect systems. The Enterprise Apps EAC reviews interconnected subservice organizations' systems' SSAE18 and Security Assessment and Authorization (SA&A) documentation: the Enterprise Apps CyberSecurity team performed a SA&A Documentation Review of the NFC Payroll/Personnel System (PPS) application in 5/2021; to review an interconnected system's FISMA status.

Complementary User Entity Controls

User entity has established controls to provide reasonable assurance that SINQ errors, HCUP Status, and mismatch cases are corrected to ensure transactions are processed correctly. The user entity has also established controls to provide reasonable assurance that data sent and received within the HRConnect system is applicable and accurate. Authorized user entities complete the Form AD-3003, Software Change Request, and submits the request to the GESD mailbox for processing when a NFC software change is applicable.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
10.1	Oracle OCI GovCloud Cloud Service Provider (CSP) Treasury Enterprise Apps reviewed the FedRAMP SA&A package and issued a Treasury Agency ATO of the OCI IaaS High GovCloud CSP.	Inquired with Enterprise Apps personnel to determine the process for monitoring Oracle OCI for compliance. Inspected the evidence of Enterprise Apps's review of	No exceptions noted.

#	Description of Controls Provided by Information Operations	Tests of Design and Operating Effectiveness Performed	Results of Design and Operating Effectiveness Testing
	Treasury Enterprise Apps monthly and annually reviews ConMon and SA&A documentation of the OCI IaaS High GovCloud CSP.	FedRAMP SA&A package to determine if OCI GovCloud has met the security requirements.	
10.2	Enterprise Apps reviews the National Finance Center (NFC)SSAE 18 report, SA&A documentation, and other subservice organization related documentation.	Inquired of Enterprise Apps personnel to determine the process for monitoring controls of subservice organizations. Inspected the evidence of Enterprise Apps's review of NFC's SSAE 18 report and SA&A documentation, and other subservice organization related documentation to determine whether the review process was followed.	No exceptions noted.

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/