JUN 2 2 2018

Approved for Release
Kevin E. Mahoney
Director for Human Resources Management and
Chief Human Capital Officer

6/22/18
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #223, FY18

SUBJECT: Guidance on the Procedures, Roles, and Responsibilities for Providing Access to HR Connect and Workforce Analytics' Applications

EFFECTIVE DATE: Upon release of this HR Bulletin

SUPERSEDES: Human Resources (HR) Bulletin #194, FY15, "Guidance on the Procedures, Roles, and Responsibilities for Providing Access to HR Connect and Workforce Analytics Systems at the Department of Commerce"

EXPIRATION DATE: Effective until superseded or revoked

REVISIONS: This bulletin incorporates the role of the Enterprise Services Organization (ESO) in the procedures, roles, and responsibilities for providing access to HR Connect and workforce analytics; replaces the previous e-mail address, HRMSProject@doc.gov, with EnterpriseServices@doc.gov; adds the Enterprise Services Contact Center and the ESO HR Portal as ways to communicate information and request assistance.

PURPOSE: This HR Bulletin provides guidance on the procedures, roles, and responsibilities for the ESO and Servicing Human Resources Offices (SHROs), who are responsible for submitting and tracking HR Connect (HRC) and workforce analytics (WA) system access requests, and assigning roles within the HR Connect system.

BACKGROUND: The ESO and each SHRO is tasked with determining the HRC and WA security access roles needed for its employees. Once determined, the ESO and SHROs must have at least one primary and one secondary security officer assigned for HRC/WA. Using the HRC and WA procedures, these security officers have the responsibility of submitting HRC and WA access requests to the Enterprise Services' Human Resources Information Technology (ES-HRIT) Team, which is the primary liaison between the Department of Commerce (DOC) and the U.S. Department of the Treasury, which hosts both systems.

COVERAGE: This bulletin applies to HR subject matter experts (SMEs), HR Specialists, and HR Assistants in the ESO and SHROs. Roles are assigned by ESO and SHRO security officers based on the job description and security clearance assigned. Since these users are assigned access by the security officers, they fall within the scope of this policy. Outside the scope of this policy are supervisory-level employees: roles for them are automatically assigned based on the "position code indicator" (manager supervisory code) associated with their specific position and

responsibilities. That role is automatically assigned to them and is not the responsibility of the security officer(s). In addition, proxies are outside the scope of this policy as they are assigned by supervisors and not by the security officer(s).

PROCEDURES: It is the responsibility of the ESO and SHROs to:

- Assign at least one primary and one secondary security officer, to ensure that security functions can continue if the primary officer is unavailable.

- Inform the ES-HRIT Team (via e-mail to EnterpriseServices@doc.gov) of any changes in security officer personnel.

It is the responsibility of the ESO and SHROs' security officers to:

- Be educated on what accesses are granted in each role when working with the HRC and WA. Contact the ES-HRIT Team for clarification when needed (refer to "HR Connect Role Assignment" on HRC's Connect-2-Learn website).

- Make appropriate adjustments to the HRC roles and responsibilities via the bureau maintenance module in HRC.

- Forward ALL system access requests to the ES HRIT Team (via an e-mail to EnterpriseServices@doc.gov). Use the current Security Access Request form when submitting system access requests. A tracking ticket will be assigned to ensure proper completion.

- Perform semiannual (Q1 and Q3) internal audits of all HRC and WA security accesses currently in effect to ensure that the level and scope of access is still valid and required. Results of the review must be sent to the EnterpriseServices@doc.gov mailbox. The ES-HRIT Team will initiate this recurring activity. This supplements the security officer's access control process that reviews and modifies access as needed (e.g., changes in responsibility for HR SMEs, new hires, and terminations) as part of the daily operational process.

- Convey Personally Identifiable Information (PII), if required, to the ES-HRIT Team by following three methods:
  1. Via direct phone interaction with the ES-HRIT Team working on the access (no PII is to be left on voicemail); or
  2. Send securely through the DOC Accellion or other DOC-approved secure file transfer to the ES-HRIT Team mailbox: EnterpriseServices@doc.gov.
  3. Send a service request securely through the ESO HR Portal (Service Now).

- Follow HRC and WA system access guidelines for security officers:
  1. Serve as the liaison between agency users and the ES-HRIT Team.
  2. Provide security awareness information to those employees who received user-access accounts to HRC or WA. Inform employees that they are to keep their user accounts safe and to not divulge their password.
  3. Submit properly completed Security Access Request forms to the

ES-HRIT Team (to EnterpriseServices@doc.gov) and make sure PII data is encrypted. If the request is for a contractor, include the expiration date.

4. Immediately suspend access to users who have separated, or as otherwise instructed, and submit a request to have those user accounts deleted (to EnterpriseServices@doc.gov).
5. Review monthly security access reports to ensure that only authorized current employees have access to agency resources and to ensure that access for separated employees has been removed. To obtain security access ad hoc reports, send a request to EnterpriseServices@doc.gov.
6. Refrain from requesting security access changes for one's own user ID.
7. For troubleshooting, call the Enterprise Services Contact Center at (888) 316-2285 or send a request to EnterpriseServices@doc.gov if you require assistance. Include the user's exact error message (provide a screenshot) if possible.
8. Attend HR Connect security officers' training as needed.
9. Users whose accounts are about to expire will be prompted when they login. After three failed access attempts, the account will be locked. Contact the Enterprise Services Contact Center to unlock an account.
10. Be sure to review and act upon security notifications.

ACCOUNTABILITY:

- The ESO and SHROs are required to provide validation that they performed the required internal review audits (the re-certification process) by sending an e-mail to the EnterpriseServices@doc.gov mailbox. The validation must consist of a narrative explaining the results, which includes at a minimum:
  - Who performed the audits;
  - When they were performed;
  - What was audited: that is, a complete list of all HR SMEs (HR Specialists and HR Assistants) checked, including any HR servicing contractors; and
  - A resolution of issues found must also be included in the validation narrative.

- Validation and results narrative must be completed by the 15th day after the end of the quarter (i.e., January 15 for Q1, and July 15 for Q3) or the next business day if the 15th falls on a non-business day to the EnterpriseServices@doc.gov mailbox.

- The ES HRIT Director will review the validation submissions to ensure completeness and to look for systemic issues that need to be addressed either DOC-wide or within the ESO/SHRO.

REFERENCES: HRC privacy and security policy can be found at: https://www.hrconnect.treas.gov/tr_images/privacy_policy.html

HUMAN RESOURCES MANAGEMENT SYSTEM: Gary Haney, HRIT Director, ghaney@doc.gov , (202) 482-1691

APPLICATION SUPPORT LEAD: Kieu (Bobby) Lam, klam@doc.gov , (202) 482-2899