AMENDMENT TO A FISH AND WILDILFE SERVICE MANUAL CHAPTER

Series: Finance
Part 260: Financial Management
Chapter 4: Retaining Financial and Business Management System (FBMS) Access, published 11/14/2021
Amendment Number: 1
Purpose: This amendment is in response to a Department of the Interior Office of Financial Management (PFM) request that all of the bureaus clarify in their policy that access to FBMS depends on four factors, and that removing any one of those factors removes access to FBMS. This amendment makes it clear that removing access can include locking users, etc., and not just removing roles or users.

Actions:

1. Change section 4.1A by striking text as shown below:

4.1 What is the purpose of this chapter? This chapter describes:

A. The U.S. Fish and Wildlife Service's (Service) requirements for employees to continue to retain access to key subsystems within the Financial and Business Management System (FBMS) ~~and for removal of end user roles~~. FBMS is the financial system of record for the Department of the Interior (Department); and

2. Add section 4.3C:

C. Factors for access. For a user to access FBMS and make changes to data, the user must have all of the following:

(1) Access to the Department's internal network,

(2) An active, unlocked Active Directory account (typically this means the user must have an active Personal Identity Verification (PIV) card),

(3) An active FBMS user ID with roles assigned to it, and

(4) An unlocked FBMS user status.

3. Update section 4.4:

- **In section 4.4A, change the following:**

FROM:

A. The Department controls the various access requirements for each non-key subsystem and works with the Joint Administrative Operations (JAO), Administrative Operations Center (AOC) Financial Systems/FBMS Operations, User Support team to identify and resolve user access issues to those systems. Some non-key subsystems may automatically lock out users after 45 days of no use, while for others it may be different.

TO:

A. The Department controls the various access requirements for each non-key subsystem and works with the Joint Administrative Operations (JAO), Administrative Operations Center (AOC) Financial Systems/FBMS Operations, User Support team to identify and resolve user access issues to those systems. The Department controls the automatic locking of accounts or subsystems. FBMS automatically locks out users after 45 days of no activity in FBMS. Some subsystems automatically lock out users after 45 days of inactivity for that subsystem, even though the user is active in other subsystems.

- **In section 4.4B(1) – (3), change the following:**

FROM:

B. For those using key subsystems that the Service controls, users must log on to and use each key subsystem for which they need access at least once every 365 days. Users do not have to use every role they are assigned within that 365 days, but they must use at least one of their roles to enter the key subsystem to retain their access. (See section 4.8 for more information about why these security requirements are in place.)

(1) FBMS users who have not accessed any key subsystem in FBMS for the previous 365 days will have all of their roles removed and their User Identification (ID) removed from all key subsystems.

(a) If the user has no remaining roles in FBMS, we will deactivate them. Deactivated users continue to retain access to some non-key subsystems that the Department controls (e.g., Tableau, uPerform, etc.).

(b) If a user receives automated report(s) from EMIS at least once every 365 days, they are considered active users in EMIS.

(2) FBMS users who access and use one key subsystem, but not another, for the previous 365 days, will retain access to the subsystem used and lose access to the unused key subsystem(s). We will remove all of their roles within the unused key subsystem(s).

(3) FBMS users who access and use one key subsystem within the past 45 days, but have not accessed another key subsystem, will retain access to the key subsystem used and may be automatically locked out of the unused key subsystem(s). All of their roles will remain intact, but they must submit a request to the FBMS Help Desk to be unlocked in the unused subsystem.

TO:

B. Users must log on to and use each key subsystem for which they need access at least once every 365 days. Users do not have to use every role they are assigned within that 365 days, but they must use at least one of their roles to enter the key subsystem to retain their access. (See section 4.8 for more information about why these security requirements are in place.)

(1) FBMS users who have not accessed any key subsystem in FBMS for the previous 365 days will be locked out of that subsystem. We will remove all of their roles and their User Identification (ID) from all key subsystems when possible.

> **(a)** If the user has no remaining roles in FBMS, we will deactivate them. Deactivation removes all roles that can enter information into FBMS.
>
> **(b)** If a user receives an automated report(s) from EMIS at least once every 365 days, we consider them active users in EMIS.
>
> **(c)** We cannot deactivate or remove some roles from users immediately because of workflow requirements (e.g., we cannot remove Contracting Officers if they have an open contract because the invoice payments on the open contract will fail). When a role cannot be removed, the FBMS user ID must be locked. After all of the workflow items that depend on the user ID are complete, we will remove the role(s). We will deactivate the user if appropriate.

(2) FBMS users who access and use one key subsystem, but not another, for the previous 365 days, will retain access to the subsystem used and lose access to the unused key subsystem(s). We will remove access to the unused key subsystem(s) and will remove roles when possible.

(3) FBMS users who access and use one key subsystem within the past 45 days, but have not accessed another key subsystem, will retain access to the key subsystem used and may be automatically locked out of the unused key subsystem(s). If they are locked out, all of their roles remain intact, but they must submit a request to the FBMS Help Desk to be unlocked in the unused subsystem.

4. Update section 4.5C by adding a "the" before "latest" and remove "s" as shown below in red font:

C. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4; Security and Privacy Controls for Federal Information Systems and Organizations; April 2013 and updated January 22, 2015 or the latest version~~s~~ of NIST SP 800-53 as it is implemented by the Department.

/sgd/ Stephen Guertin
DEPUTY DIRECTOR

Date: April 12, 2022