Attachment B

Draft Memorandum

Request for Access to Departmental HR, Payroll, and Credentialing Systems

MEMORANDUM

Subject: Request for Access to Departmental HR, Payroll, and Credentialing Systems

Department of the Interior (DOI) officials (Tyler Hassen, Stephanie Holmes, and Katrine Trampe, hereafter "requesting officials") have requested administrative/root access to the Department's Human Resources (HR), Payroll, and Credentialing systems in relation to their official responsibilities at the Department. Such elevated access to critical high-value asset systems is rare with respect to individual systems and no single DOI official presently has such access to all HR, Payroll, and Credentialing systems. This warrants consideration of consistency with DOI policy and industry best practices, particularly the principles of least privilege and separation of duties, as well as appropriate non-system mitigations. Given the nature of the system access requests and the possible implications of such access, including the risks summarized below (a more detailed risk assessment is available upon request), as well as existing Departmental policies, granting such request exceeds the authority of the Chief Information Officer. The decision to grant access, however, may be provided by the Secretary.

Risks:

Privacy and Compliance: Requested access relates to systems containing highly sensitive personally identifiable information subject to controls under the Privacy Act and other applicable authorities, the violation of which may carry criminal penalties.

Internal Control Standards: Separation of duties for users with administrative/root access consistent with NIST 800-53 standards and industry best practices preclude users from inadvertently incorrectly manipulating systems and introducing unauthorized actions (such as with respect to payment recipients). Requested access does not conform with separation of duties standards.

Interdependency and System Integrity: HR, Payroll, and Credentialing functions are interdependent. Inadvertent unauthorized or improper changes to one system could impact payroll accuracy, tax withholdings, benefits distribution, and other critical functions, leading to improper payments, financial discrepancies, and compliance failures.

Cybersecurity, Insider Threat, and Malicious Actor Concerns: Full administrative/root access enables individuals to initiate and modify personnel and payroll actions, potentially locking out other authorized users. Additionally, personnel with elevated privileges across multiple systems become prime targets for credential compromise by nation-state adversaries or other malicious actors.

Internal Control and Fraud: Internal controls and separation of duties typically advise against unchecked administrative/root access to reduce fraud risk, particularly as a result of credential loss or spoofing.

Skillset Risks: Administrative access to many of the systems typically requires training and certification. Without formal qualifications, the Department may experience significant failure because of operator error.

Decision:

The requested system access to the requesting officials is granted. This decision does not modify existing delegations with respect to the HR, personnel, or other relevant program actions supported by the relevant systems.

Approval Decision:

[_____] I Approve

[_____] I Disapprove