Summary: Audit of the Morris K. Udall and Stewart L. Udall Foundation's Information System Security and Privacy Controls

Report Date: March 06, 2026 **Report Number: 2024-CTD-043**

This summary presents the results of our audit of the Morris K. Udall and Stewart L. Udall Foundation's (the Foundation) information system security and privacy controls. The Foundation is a small Federal entity established by Congress in 1992 as an independent executive branch entity for several purposes, including increasing the awareness of the importance of the Nation's natural resources; identifying critical environmental issues; providing training and educational outreach; providing management and leadership training to Native Americans and Alaska Natives; and establishing the John S. McCain III National Center for Environmental Conflict Resolution. The Foundation's 2019 and 2024 reauthorization legislation requires our office to audit the Foundation within 2 years and 4 years of enactment, respectively.

We conducted this audit between December 2024 and August 2025 to determine whether the Foundation implemented information system security and privacy controls that adequately protect and defend the confidentiality, integrity, and availability of information processed, stored, or transmitted within the Foundation's information systems in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5.

The Federal Information Security Modernization Act of 2014 assigned responsibility to NIST to develop standards and guidance that Federal agencies are required to follow to implement an agencywide information security program that effectively manages risk to the information and information systems that support the operations and assets of the agency. Federal agencies (regardless of their size), contractors, and other sources that use or operate a Federal information system are required to follow NIST risk management standards and guidelines to develop and implement a risk-based approach to manage information security risk.

We found that the Foundation did not adequately implement privacy and security controls as required by NIST. This occurred, in part, due to staffing and budgetary resource limitations. We made 40 recommendations to improve and strengthen the Foundation's IT security program. We determined that two recommendations are significant and we will report them as such in our semiannual report to Congress in accordance with the Inspector General Act.[1]

The Foundation concurred with all 40 of our recommendations and provided planned corrective actions for their resolution. We consider all recommendations resolved and will track their implementation.

This is a summary of a report we provided to the Foundation's Board of Trustees.

[1] The Inspector General Act of 1978, 5 U.S.C. § 405(b), requires inspectors general to prepare semiannual reports summarizing OIG activities during the immediately preceding six-month periods ending March 31 and September 30. It also states that these semiannual reports shall include an identification of each "significant recommendation" described in previous semiannual reports on which corrective action has not been completed.