Summary: Evaluation of the Department of the Interior's Cyber Threat Hunting Program

Report Date: August 22, 2025 **Report Number: 2023-CTD-039**

This summary presents the results of our evaluation of the U.S. Department of the Interior's (DOI's) progress in establishing an enterprise-wide cyber threat hunting program. We conducted this evaluation to determine whether DOI established a cyber threat hunting program and, if so, determine its level of maturity.

Federal law, mandates, and cybersecurity frameworks require Federal agencies to establish and implement cyber threat hunting capabilities. This requirement is a core component of a broader strategy to improve the Federal Government's ability to proactively defend against increasingly sophisticated cyber threats. As cyber threats continue to evolve, these capabilities are considered critical for maintaining national security and protecting Government data and infrastructure. Without a mature enterprise threat hunting program and related capabilities, cyber adversaries may remain undetected for prolonged periods of time before discovery, placing DOI sensitive data and mission operations at high risk of loss or disruption.

We made three recommendations to improve DOI's enterprise-wide threat hunting capability and strengthen DOI's IT security program.

We recommended that the OCIO:

1. Develop and implement policies, processes, and procedures to be followed by Cybersecurity Division staff who perform enterprise threat hunting activities.
2. Formally document the roles, responsibilities, and authorities of Cybersecurity Division staff and contractors who perform threat hunting activities.
3. Design and implement an enterprise-wide threat hunting program based on a recognized threat hunting framework that addresses Federal requirements and guidance.

The OCIO concurred with all three of our recommendations and provided planned corrective actions for their resolution. We consider all recommendations resolved.

This is a summary of a report we provided to the U.S. Department of the Interior.