U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

May 7, 2021

The Honorable Deb Haaland
Secretary
U.S. Department of the Interior
1849 C St., N.W.
Washington, D.C. 20240

Re: OSC File No. DI-21-000420
Referral for Investigation--5 U.S.C. § 1213(c)

Dear Secretary Haaland:

I am referring to you for investigation a whistleblower disclosure that officials at the Department of the Interior (DOI), [redacted] Planning and Performance Management Division, Washington, D.C., engaged in actions that constitute a violation of law, rule, or regulation and gross mismanagement. A report of your investigation of these allegations and any related matters is due to the Office of Special Counsel (OSC) on July 6, 2021.

[redacted], an Audit and Compliance Analyst, who consented to the release of his name, disclosed that [redacted] officials do not comply with information system security control requirements. The allegations to be investigated include:

- [redacted] officials have not documented or implemented security controls for the agency's [redacted] and other General Support Systems (GSS) as required by the Federal Information Security Management Act of 2002 (FISMA)[2], leaving DOI's systems vulnerable to security threats; and
- Any additional, related allegations of wrongdoing discovered during the investigation of the foregoing allegations.

[redacted] disclosed that [redacted] officials have not ensured that security controls for [redacted] are properly implemented or documented in DOI's Cybersecurity Assessment and Management (CSAM) database.[3] According to [redacted], pursuant to OCIO Directive 2011-006, [redacted] CSAM entry must include documentation reflecting that required controls are in place for the system, including a system security plan and an authorization to operate (ATO). According to [redacted], [redacted] CSAM entry lacks nearly all of the necessary

[redacted]

[2]44 U.S.C. § 3541–48 (2008); *See* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Rev. 1, para 1.1 (February 2006). "[FISMA] requires federal agencies to develop, document, and implement an agency-wide information security program..."
[3]CSAM is a tool that allows agencies to track and manage information systems and associated security vulnerabilities and collect data to facilitate FISMA reporting.

documentation, indicating that the system is not properly secured. For example, [redacted] disclosed that CSAM does not contain a system security plan for [redacted] which is required for all information systems and, according to [redacted] must be one of the first documents generated when building a new system.[4] Although CSAM does not reflect any of the required documentation, [redacted] disclosed that CSAM contains a September 10, 2020, ATO signed by [redacted] stating that she reviewed [redacted] security controls and authorized its operation. [redacted] alleged that this determination is not possible because [redacted] lacks all of the security documentation required for an authorization review.[5]

[redacted] further disclosed that [redacted] officials rated [redacted] as a low impact system containing no personally identifiable information (PII) and categorized it as "developmental" for at least three to four years, despite being a fully operational system.[6] [redacted] noted that [redacted] officials also identified [redacted] as not "FISMA-reportable"—a status that is not defined by FISMA—which [redacted] officials use to avoid accountability for failing to secure and maintain the system. [redacted] further disclosed that [redacted] is a "parent" system for other systems that are rated moderate impact, which permits [redacted] officials to also avoid submitting FISMA reports for these systems. [redacted] alleged that these deficiencies leave DOI information technology systems at risk of threats and exploits akin to the 2020 SolarWinds hack.[7]

I have concluded that there is a substantial likelihood that the information provided to OSC discloses a violation of law, rule, or regulation and gross mismanagement. Please note that specific allegations and references to specific violations of law, rule or regulation are not intended to be exclusive. As previously noted, your agency must conduct an investigation of these matters, and I will review the report for sufficiency and reasonableness before sending copies of the agency report along with the whistleblower's comments and any comments or recommendations I may have, to the President and congressional oversight committees and making these documents publicly available.

Additional important requirements and guidance on the agency report are included in the attached Appendix, which can also be accessed at https://osc.gov/Services/Pages/DU-Resources.aspx. If your investigators have questions regarding the statutory process or the report required under 5 U.S.C. §1213, please contact Catherine A. McMullen, Chief, Disclosure Unit, at (202) 804-7088 for assistance. I am also available for any questions you may have.

Sincerely,

Henry J. Kerner
Special Counsel

Enclosure
cc: The Honorable Mark Lee Greenblatt, Inspector General

---

[4]*See* NIST SP 800-18, Rev. 1 at para. 1.5, "All information systems must be covered by a system security plan…"
[5]Office of Management and Budget (OMB) Circular A-130, para 10.a.(8)
[6]Federal Information Processing Standards Publication 199, para. 3. (February 2004) defines three levels of potential impact on organizations or individuals in the event of a security breach: low, moderate, and high.
[7]Dina Temple-Rastin, *The SolarWinds Attack: The Story Behind The Hack* (April 20, 2021) *available at* https://www npr.org/2021/04/20/989015617/the-solarwinds-attack-the-story-behind-the-hack.