United States Department of the Interior
OFFICE OF THE SOLICITOR
Washington, D.C. 20240

March 11, 2022

The Honorable Henry Kerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, D.C. 200036

Re: OSC File No. DI-21-000716

Dear Mr. Kerner:

The Department of the Interior ("Department" or "Interior") writes to provide a response to your August 27, 2021 referral (OSC file no. DI-21-000716) of a whistleblower disclosure for investigation by the Secretary of the Interior. This referral was joined with a previous referral your office sent on May 7, 2021, (OSC file no. DI-21-000420) which involves the same whistleblower.

This letter responds to the allegations raised by the whistleblower in DI-21-000716 and informs your office of steps that the Department has taken to review the allegations your office referred. Further, this letter articulates why the Department believes that OSC should instead engage with the General Services Administration ("GSA").

U.S. OFFICE OF SPECIAL COUNSEL REFERRAL (OSC File No. DI-21-00716)

On, August 27, 2021, your office referred DI-21-000716, which contained allegations related to a "DOI" information technology ("IT") system called FOLIO. According to the whistleblower, FOLIO is "a web-based, Government-owned Software-as-a-Service (SaaS) technology solution that Federal Agencies use to support their internal portfolio management, IT capital planning, and IT Governance processes to meet their external report requirements to the Office of Management and Budget."

The whistleblower made two overarching allegations concerning FOLIO. First, the whistleblower alleged that FOLIO is improperly marked as not Federal Information Security Management Act ("FISMA") reportable and that DOI has purposefully marked it as such to avoid submitting FISMA reports for the system, thereby posing a security threat to the Department's IT systems. Second, the whistleblower alleged that FOLIO's Cyber Security Assessment and Management ("CSAM") entries contained contradictory and incomplete information. The whistleblower provided a specific example where FOLIO is identified in CSAM as a "non-financial" system, but the CSAM "Information Types" page includes several security categorization ratings for FOLIO's financial capabilities.

FISMA ALLEGATION

FOLIO is a General Services Administration System and not a Department of the Interior System.

FOLIO is a web-based, government-owned fee-for-service technology solution that federal agencies use to support their internal Portfolio Management, IT Capital Planning, and IT Governance process to meet their external reporting requirements to the Office of Management and Budget. FOLIO is provided by GSA Office of Government-wide Policy and was designed by the Federal ePIC Steering Committee ("FESCOM"). The FOLIO system is used by 17 federal agencies, including the U.S. Office of Personal Management, U.S. Department of Justice, and the National Archives and Records Administration. GSA is the agency that appropriately maintains the capital investment for FOLIO (see Agency Summary - General Services Administration | IT Dashboard for "Investment UIID 023-999993310 General Activities Government-wide Folio Program"), reports FOLIO as part of its system inventory under FISMA, and issues the Authorization to Operate ("ATO") for FOLIO as required by OMB Circular No. A-130. FOLIO is not operated by or under the control of DOI, however it does include DOI information pursuant to the GSA-issued ATO.

Legal Requirements Under the Federal Information Security Modernization Act

Pursuant to 44 U.S.C. § 3505(c)(1) "[t]he head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) *operated by or under the control of such agency*." (emphasis added). As such, an agency that leverages a system but does not operate or control the system may designate the system as "not FISMA Reportable" because it is not that agency's responsibility under the relevant statues to designate it as such.

Under 44 U.S.C. § 3554(c)(1)(A)(iv), the Director of the Office of Management and Budget (OMB) and the Secretary of Homeland Security are empowered to require that "any other information" in addition to statutorily required elements be included in annual agency reports on "the adequacy and effectiveness of information security policies, and practices that are required by U.S.C. § 3554(c)(1)(A). Each year, OMB and the Department of Homeland Security ("DHS") collaborate to issue "CIO FISMA Metrics" that provide agencies with guidance on the specific information required to be reported for that year. The reporting guidance annually includes a requirement for agencies to report "the number of operational unclassified information systems". *See CIO FISMA Metrics FY 2022.*

Authorization to Use

OMB has directed agencies to adhere to guidance issued by the National Institute of Standards and Technology ("NIST") with regard to securing information and information systems. NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," introduces an additional system authorization called "Authorization to Use" ("ATU"). Per that document, "[a]n authorization to use is employed when an organization (hereafter referred to as the

customer organization) chooses to accept the information in an existing authorization package produced by another organization (either federal or nonfederal) for an information system that is authorized to operate by a federal entity (referred to as the provider organization). The term provider organization refers to the federal agency or subordinate organization that provides a shared system, service, or application and/or owns and maintains the authorization package (i.e., has granted an Authorization to Operate for the shared system, service, or application)."

Application of the Federal Information Security Management Act to FOLIO

By practice, the Department excludes all systems for which it maintains an ATU from its reportable system inventory. To do otherwise would falsely inflate the number of information systems operated across the federal government, since an agency that issues the ATO must include the system in its reportable system inventory under FISMA. As noted above, GSA maintains the capital investment for FOLIO and reports FOILIO as part of its system inventory under FISMA. In this instance, GSA is the provider organization that provides the FOLIO system and has issued the ATO. DOI, as a customer organization, has issued an ATU for the FOLIO system in accordance with the NIST guidance and its own policy implementing that guidance. The current DOI ATU for FOLIO has an expiration date of September 22, 2023. DHS confirmed this practice is appropriate in an email to DOI, which further stated that it is appropriate for an agency that issues an ATU to a system to exclude such system from the FISMA reportable inventory.

General Service Administration FISMA Responsibilities for FOLIO

As articulated above, since FOLIO is not a DOI-controlled or operated system, DOI has no obligation to report the system as a FISMA reportable system. Rather, GSA, as the owner and operator of the system, would be the only government agency that could and would be responsible for listing the system as FISMA reportable. DOI merely possesses an ATU. If the whistleblower feels that FOLIO is not being properly listed as a FISMA reportable system, that responsibility would lie with GSA and any allegation regarding FISMA reportability could only be addressed and investigated by the GSA.

CSAM Allegation:

CSAM Entries are Based on Information Provided By the General Services Administration

The CSAM system is DOJ-created and owned and provides a secure web-based platform for maintaining an inventory of IT systems and security boundaries, and for maintaining security data and documentation related to the registered systems and DOI security programs.

For reasons of operational efficiency, DOI chooses to maintain information on systems that do not meet the threshold for inclusion in the annual FISMA report within the same repository system that holds the data on systems that do not meet the FISMA reportable threshold. These include systems that are not in an operational state (e.g., systems that are under development), as well as systems that are no longer operating but for which records must be retained to meet records management requirements. Also included in CSAM are records of systems that are not

operated by or under the control of DOI, which the agency tracks for the purpose of complying with requirements around data management, such as FOLIO. While DOI does not operate or control those system, those systems generally contain DOI information and thus are tracked with the CSAM system.

How the Department catalogs FOLIO in CSAM is based on information provided by or derived from GSA. As mentioned above, GSA is the owner and operator of FOLIO and, pursuant to FISMA, is the agency responsible for reporting the system. All information, data, and definitions concerning FOLIO are provided by GSA. As such, the Department's CSAM entries concerning FOLIO are derived from the information provided by the GSA. GSA is the only entity with the necessary documentation and information to properly support the FOLIO system as required by Federal information security laws. Specifically, as noted above, under FISMA it is the owning/operating agency that is responsible for classifying the system as either FISMA reportable or not reportable and providing the necessary classifications and supporting documentation. As an authorized user of the system, DOI is not in possession of any information other than that which is provided by GSA, and thus, the information in CSAM is derived only from the information that GSA has provided. GSA is responsible for ensuring that such information is sufficient and in no way redundant, lacking, or faulty. Indeed, GSA is the only federal agency capable of determining the sufficiency of such information. It would then be GSA's responsibility to inform an agency with an ATU, such as DOI, that various determinations have been made or relevant artifacts created, corrected, or removed.

CONCLUSION:

The allegations referred to the Department by your office can only be addressed by the GSA. The FOLIO system is a GSA owned and operated system for which the Department has a properly executed ATU. Because the Department does not own or operate FOLIO, it is not responsible for reporting the system under FISMA. That determination and responsibility lies with the GSA. Additionally, all information and characterization of the system within the Department's use of CSAM is based on documentation and information provided by or derived from the GSA. The GSA bears responsibility for providing accurate and updated information to the federal agency with an ATU.

Our conclusion that GSA is the proper agency to address the allegations your office referred to the Department is bolstered by the Offices of Inspectors General ("OIG") for both the Department of Justice and the Department of Education. After it was determined that the OIG for Interior should not conduct an investigation into this matter, we inquired with the OIGs for Education and Justice. Both OIG declined to investigate the matter on our behalf as they believed the system was controlled and operated by GSA.

If you have any further questions or concerns, please reach out directly to Jeffrey Scott, Attorney-Adviser, Office of the Solicitor at (202) 513-0512 or at Jeffrey.Scott@sol.doi.gov.

Sincerely,

SCOTT DE LA VEGA

Digitally signed by SCOTT DE LA VEGA
Date: 2022.03.11 13:41:19 -05'00'

Scott A. de la Vega
Associate Solicitor for General Law