July 13, 2022

To : Siobahn Bradley

OSC Investigator

From : [redacted]

CAM FISMA IT Security Audit and Oversight Compliance

Re : Amended; Whistleblowers response to agency's reply to OSC File No. DI-21-000716

Whistleblower response and comments to the Department of the Interior referral OSC file no. DI-21-000716 of a whistleblower disclosure of violations of laws, rules and regulations specifically FISMA 44 USC 3554 for the FOLIO systems referred for investigation by the Secretary of the Interior. The response is signed by high-ranking DOI official, the Associate Solicitor for General Law who is notably not a FISMA nor IT Security professional but may act as a legal shield for the DOI[redacted] and OIG. The agency response admits that FOLIO "*generally contain DOI information*" but also admits that it neglected to properly investigate the allegations yet it indirectly and circuitously commented on two of its broad summarizations of the allegations. Its response simply deferred the allegations to GSA and the agency averse that it had no liability nor culpability because FOLIO is a GSA owned and operated system although it simultaneously admits that FOLIO "*generally contain DOI information*". The agency fails to cite or admit that FOLIO is in fact a shared-system with shared FISMA responsibilities and is governed by FedRAMP. FedRAMP implements FISMA and NIST requirements through federal cloud-based shared resources including FOLIO. The agency response consistently fails to provide evidence, documentation, citations or hyper-links to any supporting or corroborating testimony or response. While none of its comments directly addressed or responded to the allegations many were found to be false, conclusory, unsubstantiated and in some instance counter-evidenced. By ignoring FedRAMP governance the agency fails to take ownership for any deficiencies specific to FOLIO and pushes them off to GSA. The agency also fails to directly cite deficiencies or allegations specific to mandated FISMA documentation, or the lack there-of as cited in the whistleblowers protected submission.

The Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554) requires the head of each Federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise. Since FY 2016, OMB and the Department of Homeland Security (DHS) have organized the CIO FISMA metrics around the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The FISMA metrics leverage the Cybersecurity Framework as a standard for managing and

reducing cybersecurity risks, and they are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework, when used in conjunction with NIST's 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems, 800-39, Managing Information Security Risk: Organization, Mission, and Information System View and associated standards and guidelines, provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their enterprise. The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information. FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies (https://www.fedramp.gov/program-basics ). The agency failed to provide any evidence that it satisfied these laws and requirements and its response to the allegation also failed to address the laws and requirements.

The agency response is signed by a high-ranking DOI official, The Associate Solicitor for General Law and failed to refute or contest any of the allegations or evidence cited in the whistleblowers protected submission which included [redacted]. Despite the agency admitting that FOLIO "*generally contain DOI information*", the agency failed to address, refute nor explain how or why FOLIO' CSAM presence began with deceptive, misleading or false inputs and data for instance; although FOLIO was listed as a "Non-Financial" system its CSAM "Information Types" page indicates several Security Categorization ratings for FOLIO' financial capabilities and the eCPIC CSAM homepage states that FOLIO replaces eCPIC' mission function and capabilities (see also https://gsablogs.gsa.gov/folio/2017/11/03/folio-evolution/). eCPIC is a known and recognized Financial system and had additional OMB mandated IT Security responsibilities and requirements for a Financial system accordingly, FOLIO seems to be circumventing, evading or violating those OMB responsibilities and requirements by pretending\purporting to be "Non-Financial" as reported in the whistleblowers protected submission which included CAM System, Application or Network FISMA IT Compliance Measures, Audit and Review For FOLIO, 07-15-2021. The agency response failed to address, refute or explain how or why FOLIO was reported and evidenced with a series of invalid [redacted] with repeatedly unmet and unsatisfied terms, requirements and conditions, signed by high-ranking [redacted] officials. [redacted]. The agency response failed to address, refute or explain how or why the two uploaded FOLIO [redacted] signed by the Authorizing Official and [redacted] PPMD Chief , [redacted] And the agency's response failed to address, explain or even refute why or how none of the DOI\[redacted]

dangerous IT Security practices are not being or has been reported to OMB, GAO or to Congress for over five years if ever; instead they create a ruse about contacting OIGs external to DOI and claim "it aint ours so go tell GSA" while simultaneously admitting that FOLIO "*generally contain DOI information*". Without any explanation, investigation, documentation or evidence to refute the allegations of violations of laws (44 USC 3554), rules and regulations nor a simple and plain refutation or denial, an outside objective observer is left to conclude that each and every allegation is verified and true. Furthermore prior protected activity and OIG reports corroborates the whistleblowers allegations and indicates that the FOLIO violations are a long and ongoing culture at DOI[redacted] propagated, directed and extended by its highest ranking [redacted] managers such as the [redacted] PPMD Chief and the PDCIO and protected by DOI highest-ranking Officials such as the Associate Solicitor for General Law, with an immunity to correction.

[redacted]

[redacted]