July 12,2022

To : [redacted]

OSC Investigator

From : [redacted]

[redacted]CAM FISMA IT Security Audit and Oversight Compliance SME

Re : Whistleblower comments for OSC complaint DI-21-000420

DOIOIG Federal Information Security Modernization Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2021 Report 2021-ITA-037 made 60 Recommendations. The report cited the [redacted] 81 times and specified [redacted] 28 times. The report shows that of the 12 DOI systems audited [redacted] was the worst or had the most findings, deficiencies and recommendations.

On the day of the FISMA IT Security Oversight Audit and Review [redacted] gap-analysis and revisit [redacted] was found to be Materially Deficient and dangerously non-compliant with FISMA laws (Public Law 113-283, 44 USC 3554), NIST regulation, DHS\CISA requirements, OMB, GAO and OIG findings and recommendations, DOI Policy and common and accepted standards of basic IT Security practices and principals. [redacted] as observed at the time of this oversight review supports, represents and evidences the findings in the prior oversight reports cited above while [redacted] systemic and embedded non-compliant practices and methodology ensures the proliferation, continuance, cover-up and protection of the kind of violations, findings and outcomes cited in the oversight reports by GAO, OIG and OSC reports File Nos. DI-17-004363, DI-21-000420 and DI-18-001324. This review found repeated and systemic violations of laws, regulation, rules and policies at nearly every stage of the [redacted] FISMA and IT Security controls assessment, authorization and remediation reporting including false\fraudulent reporting to OIG and federal oversight.

The whistleblower has lawfully reported [redacted] on multiple occasions for repeated Material Deficiencies in its IT Security and FISMA compliance practices including OSC complaint DI-21-000420. By February of 2021 the DOIOIG contractors completed its audit of [redacted] and found numerous IT Security and FISMA deficiencies that was congruent with and supported those reported by the whistleblower. The OIG audit neglected to review key mandated FISMA documentation such as the ATO, the SSP, the CP or inspect a sample of the POA&Ms nor assess them for veracity, relativity, or compliance. The agency failed to dispute, contest or provide any evidence to refute, contest or rebutt the allegations cited OSC complaint DI-21-000420 or that [redacted] lacked a compliant [redacted], [redacted] as mandated by FISMA , Public Law 113-283, 44 USC 3554. The **OIG FISMA Performance Audit Report, 2021-ITA-037** also failed to find any evidence to refute, contest or rebutt the allegations cited by the whistleblower in OSC complaint DI-21-000420 but

conversely established sufficient, abundant and copious evidence to support and verify the allegations cited by the whistleblower in OSC complaint DI-21-000420.

All of OCIOLAN's nefarious and non-compliant IT Security practices are executed with no POA&Ms and no recorded budget for POA&Ms and vulnerability remediation thereby creating a seeming "windfall" for DOI which support the findings cited in GAO Report GAO-18-42; " DOI did not properly identify almost 50 percent, or $292 million, of its IT contract obligations in FY 2016". None of the dangerous practices are being or has been truthfully reported to OMB, GAO or to Congress for over five years if ever; the potential risk from [redacted] serial, embedded and repeatedly deficient FISMA and IT Security practices to all DOI employees, [redacted] Pursuant to the October 11, 2019 [redacted] *of the* [redacted] memorandum the CAM branch and the PDCIO are responsible for the systemic and programmatic false reporting to OMB, GAO, Congress and OIG and have been evidenced and reported to multiple authorities including OSC File Nos. DI-17-4363 and DI-18-1324 on numerous occasions of routinely violating, circumventing or ignoring multiple laws, rules or regulations and\or abusing their authority specific to IT Security and FISMA as well as attempting to "cover-up" the reported abuses. The OSC found [redacted] responses, testimony and explanations by then CISO, the PDCIO the CAM chief and [redacted] managers as "not credible", they circumvented accountability during the investigation of OSC complaint # DI-21-000716 simply by having the DOI Deputy Solicitor who has no IT Security nor FISMA expertise sign or "hand over" the agency response to the allegations in what was clearly a "cover" for [redacted] This and previous FISMA IT Security Audit and Oversight reviews evidence that [redacted] and numerous other [redacted] owned, operated or managed systems, applications and [redacted] and others routinely engage in FISMA violations and false reporting to oversight including Congress. The previous CIO had addressed these deficiencies by assigning blame to the DAS\AS via the [redacted] but the deficiencies in [redacted] persisted.

Top [redacted] Managers such as the [redacted] routinely executing illegal practices (44USC3554) is not a first (see OSC File Nos. DI-17-4363 and DI-18-1324) nor an uncommon finding in [redacted] but it is illegal, dangerous and has all of the hallmarks or potential impact of a high-level insider threat. [redacted] has been reported in over 40 FISMA IT Security Audit and Oversight reviews (REVAMP) as operating a systemically, programmatically and ongoing non-compliant, defiant or illegal IT Security program and FISMA practices, as reported in OIG Report No.: 2019-ER-052 which states; "*After 7 years, the DOI has not fully implemented Phase 1 of the Continuous Diagnostics and Mitigation (CDM) program, a cybersecurity approach to fortifying networks that began in 2012. We previously found that for all four CDM Phase 1 controls the bureaus either failed to implement the control or the control was implemented incompletely or ineffectively*" are lead, supported, executed and \or protected by the highest officials in [redacted] which presents an ongoing danger and threat to DOI while apparently losing, wasting, re-directing, mis-directing, stealing, or not accounting for tens of millions of dollars of [redacted] approved budget. The ongoing, embedded and systemic IT Security and FISMA violations are an apparent coordinated cover-up or a "bumbling-idiot, 3-stooges" routine to hide the fiscal improprieties, violations or crimes. The apparent objective goes beyond ongoing, persistent and tenacious FISMA and IT Security incompetence but

indicates a bigger violation or crime such as intentional loss, mis-appropriation, mis-direction, re-direction or theft of federal funds consistent with the findings cited in GAO Report GAO-18-42; " *DOI did not properly identify almost 50 percent, or $292 million, of its IT contract obligations in FY 2016*".

GAO-18-93 report dated August 2018 identified numerous IT deficiencies; In compliance with FISMA (44USC3554) which states, *"(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions"* and the CIO to *"have a significant role in (1) budgeting decisions and (2) the management, governance, and oversight processes related to IT"*. [redacted] and [redacted] has been evidenced routinely neglecting to report and\or intentionally mis-reporting (falsifying) its [redacted] while simultaneously submitting skewed, misleading or false reports of its remediation efforts to outside oversight to include GAO, OMB, OIG and reports to Congress. The scale of these ongoing and systemic violations and crimes are dire and [redacted] as observed in CSAM on the day of this Audit and Review evidences that [redacted] while the CIO CISO and PDCIO continues to fail to satisfy and remediate the findings cited in several Oversight reviews and reports to include OIG, GAO and OMB thereby creating and sustaining a Materially dangerous IT environment and culture for DOI , its IT connected peers and national.

[redacted] was reported in OSC complaint DI-21-000420 and the Summary of Findings discovered during this Audit and Review that it continues to suffer from the following law violations, deficiencies and Material Weaknesses ;

1. [redacted] continues operating in an illegal and non-compliant manner in violation of FISMA regulation, [redacted], DHS\CISA requirements and DOI policy since circa 2017
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]
8. The [redacted] violations and non-compliant conditions continues to be not reported to OIG, OMB, GAO or Congress oversight as required

[redacted]