Federal Election Commission
Office *of the* Inspector General

MEMORANDUM

TO: The Commission

FROM: Christopher Skinner
Inspector General

SUBJECT: FEC OIG Open Recommendations Snapshot – Oversight.Gov

DATE: February 16, 2022

ENCL: (1) FEC OIG Open Recommendations Snapshot

This memorandum transmits the Office of Inspectors General's (OIG) snapshot of FEC open recommendations as of February 2022. As required by the Inspector General Act of 1978, (IG Act), the OIG is responsible for, among other things, conducting and supervising audits and investigations that recommend improvements to the FEC's programs and operations.

The enclosed snapshot is available to the public on Oversight.gov and can be exported at any time. Accordingly, we intend to keep this information accurate and current. The snapshot contains embedded weblinks to the accompanying OIG reports with detailed descriptions of each recommendation.

The IG Act further requires the OIG to conduct follow-up assessments and report to Congress on the status of open OIG recommendations. The OIG collaborates with management to develop actionable and mutually agreeable recommendations. Management may take three courses of action to address OIG recommendations:

1. Management may implement the corrective action recommended by the OIG;

2. Management may determine to address the recommendation by another means; or

3. Management may determine no corrective action is warranted and/or accept the risk. If so, management should provide a written explanation to the OIG.

The OIG will close a recommendation once it has reviewed and verified that management's corrective action(s) have been adequately implemented to address the recommendation. In accordance with the IG Act, we are required to report open recommendations in our semiannual report to Congress. In addition, we will periodically provide an updated snapshot to the Commission and agency senior leaders for situational awareness and to promote the timely implementation and closure of OIG recommendations.

Should you have any questions regarding this snapshot, please contact me at cskinner@fec.gov. In addition, please don't hesitate to contact one of our senior auditors (Michael Mitchell at mmitchell@fec.gov or Shellie Purnell-Brown at spurnell-brown@fec.gov) for clarification on any open recommendation. Thank you.

cc: Alec Palmer, Staff Director/Chief Information Officer
Lisa Stevenson, Acting General Counsel
John Quinlan, Chief Financial Officer
Kate Higginbothom, Deputy Staff Director for Management and Administration
Greg Baker, Deputy General Counsel
Gilbert Ford, Deputy Budget Director

1	Review all current agency systems that require PIV card login and verify the fields that are used for authentication with third-party providers.
2	Verify with the PIV card issuer that all fields used for authentication in agency systems are unique after any upgrade to the software associated with issuing PIV cards.
3	Include the Chief Information Security Officer or other technically qualified IT personnel in the procurement process to determine how the third-party providers grant FEC employees' access to their systems and determine how these systems may affect FEC operations.
4	Ensure there is a formal process to memorialize the actions taken by the FEC or its contractors when there is a change from the statement of work.
5	Evaluate the services the contractor is currently providing for the PIV cards and issue a modification to the task order detailing the change in the worksite location.
2020-01	2020-01 We recommend the FEC OCIO in conjunction with the direct managers perform and document periodic user access reviews for FEC systems according to the agency's system security plan.
2020-03	We recommend the FEC OCIO utilize lessons learned from the COVID- 19 pandemic to determine if any revisions are need to the Continuity of Operation Plan, and schedule periodic testing.
2020-04	We recommend that the FEC develop system- specific contingency plans, as appropriate for the agency risk level. (Repeat Recommendation)
2020-05	We recommend the FEC OCIO implement an effective procedure to enforce compliance with the security awareness training policy to ensure all system users complete security training in accordance with the FEC Security Training and Awareness Policy.
1	We recommend the FEC DATA Act program team coordinate with the FSSP to correct errors identified in DATA Act File C submission, as well as to come to a mutual agreement how IAAs should be reported.
2	We recommend that the FEC's SAO and FSSP SAO collaborate to ensure going forward, adequate time is provided to identify and correct errors prior to the final DATA Act submission due dates.
2	The OIG recommends that the Commission update the relevant standards to clarify the criteria used to identify potential violations and provide measurable standards concerning the review of inaugural committee reports.
3	The OIG recommends that the Commission update the inaugural committee review process.
4	The OIG recommends that RAD memorialize a policy concerning the identification of potential foreign donations and that the Commission consider updating relevant forms and instructions to ensure filers are aware of verification requirements imposed by federal regulation.
5	The OIG further recommends that RAD's policy include specific thresholds that will trigger the issuance of requests for additional information (RFAIs) for donations with foreign addresses, notwithstanding purported verification by the relevant committees (political and inaugural).
1	That FEC regularly request, retrieve, and review monthly TRANServe subsidy benefit reports from the DOT in efforts to monitor benefit usage and prevent fraud, waste, and/or abuse of government funds.
2	That FEC management incorporate guidance into Commission Directive 54 that addresses transit benefits for furloughed and non-furloughed employees in the event of a government shutdown.
3	That FEC management include specific guidance related to the use of transit benefits during a government shutdown within the annual transit recertification application and within the agency PowerPoint training.
25	OHR should periodically (at least annually) review all HR- related policies and procedures for the agency and for the OHR to ensure policies and procedures are accurate and relevant, and update as needed.
11	Procure the necessary hardware/software to fully test the data entry application needed for Disclosure by December 2013.
12	Ensure the disaster recovery Kofax server is updated to mirror the Kofax production server by June 2013.
2b	Comply with OMB memoranda, or in the event of statutory exemption and a decision not to voluntarily comply, document that sufficient controls exist to mitigate the need to comply. Where compliance is not adopted due to resource constraints or other reasons, document the legal assessment, risk analysis, and cost-benefit to the FEC.
2c	Identify and implement a governance framework (e.g., NIST, the AICPA's Generally Accepted Privacy Principles (GAPP)), to ensure that controls within the FEC to protect PII are appropriately identified, documented, and implemented.
4d	Complete Phase 2 and Phase 3 of the "FEC's Plan to Review and Reduce Holdings of Personally Identifiable Information and Eliminate Unnecessary Use of Social Security Numbers In Response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information" as soon as practical. This can be accomplished by providing the STSI results to the divisions and requesting a response on the ability to reduce or eliminate the questionable uses of social security numbers already identified by the contractor.
5a	Conduct a risk assessment annually for all existing and new applications that collect, process, transmit or store PII. If PIAs were performed, a risk assessment component could be built into that process to accomplish both the PIA and risk assessment recommendations.
5b	Prepare a documented corrective action plan for any deficiency noted for each risk assessment performed and report progress periodically until all corrective actions are implemented. The corrective action plan should be approved by management.