



EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

OFFICE OF INSPECTOR GENERAL

**SEMIANNUAL REPORT TO THE U.S.
CONGRESS**

April 1, 2024 – September 30, 2024



OIG VISION

Effective, efficient, and accountable oversight of Agency programs, operations, and personnel

OIG MISSION

To detect and prevent waste, fraud, and abuse and promote economy, efficiency, and effectiveness in the programs and operations of the Equal Employment Opportunity Commission

CORE VALUES

Integrity Accountability Excellence
Collaboration Innovation

Table of Contents

MESSAGE FROM THE INSPECTOR GENERAL	3
EXECUTIVE SUMMARY	4
Completed Audit Activity	4
Ongoing Audit Activities	4
Completed Other Audit Activities.....	4
Completed Evaluation Activities	4
Ongoing Evaluation Activities	4
Completed Other Evaluation Activities	4
Ongoing Other Special Projects	4
Completed Investigative Activities	5
Ongoing Investigative Activities.....	5
INTRODUCTION.....	6
THE AUDIT PROGRAM.....	7
Completed Other Audit Activity	7
Ongoing Audit Activities	7
Completed Other Audit Activities.....	8
Other Ongoing Audit Activities	8
The Evaluation Program.....	9
Completed Evaluation Activities	9
Ongoing Evaluation Activities	9
Completed Other Evaluation Activities	10
OTHER SPECIAL PROJECTS.....	10
Ongoing Special Projects Activity	10
AUDIT AND EVALUATION FOLLOW - UP	11
Audit and Evaluation Reports Issued During This Reporting Period	11
Recommendations for Which Corrective Actions Have Not Been Completed	11
Audit and Evaluation Reports Which no Management Decision has been Made by the End of the Reporting Period.....	23



THE INVESTIGATION PROGRAM 24

 Office of Inspector General Hotline..... 25

 Closed Investigative Activities..... 25

 Ongoing Investigative Activities..... 25

APPENDICES 26

 Appendix I. Final Audit/Evaluation/Inspection Reports..... 26

 Appendix II. Investigative Statistical Report 26

 Appendix III. A Report on Each Investigation Conducted by the Office Involving a Senior
 Government Employee Where Allegations of Misconduct Were Substantiated. 27

 Appendix IV. A Detailed Description of Any Instance of Whistleblower Retaliation..... 27

 Appendix V. A Detailed Description of Any Attempt by the Establishment to Interfere with
 the Independence of the Office of Inspector General. 27

 Appendix VI. Detailed Descriptions of the Particular Circumstances..... 28

 Appendix VII. Significant Management Decision(s) 28

 Appendix VIII. Index of Reporting Requirements..... 29

 Appendix IX. Single Audit Act Reporting..... 32

 Appendix X. Peer Review Reporting..... 32



MESSAGE FROM THE INSPECTOR GENERAL

I am pleased to submit our Semiannual Report to the US Congress, summarizing the work and accomplishments of the Equal Employment Opportunity Commission (EEOC), Office of Inspector General from April 1, 2024, to September 30, 2024.

During this reporting period, the OIG continued to accomplish its primary objective to detect and prevent fraud, waste, and abuse within the EEOC.

I am quite proud to announce that our office has issued its latest Strategic Plan for FY 2024 - 2028. In developing this strategic plan, we aligned our goals and objectives with the intent of the Government Performance and Results Act of 1993 and the Government Performance and Results Act Modernization Act of 2010. We partnered strategically with our internal and external stakeholders to assist in the identification of innovative approaches and methods to help enhance the Agency's program and operational effectiveness and efficiency. We will continue to work internally in our office and with our external stakeholders to identify areas of change associated with mission attainment and strategic vision.

I would like to thank the OIG's dedicated team of talented professionals. Their resilience and flexibility during the reporting period allowed the OIG to continue its vigilance in detecting and preventing waste, fraud, abuse, and enhancing effectiveness and efficiency in the Agency's operations and programs.

Finally, I would also like to thank Chair Burrows, the EEOC Commissioners, senior Agency leadership, and their staff for their ongoing cooperation and Congress's continuing support of the OIG's mission.

Respectfully Submitted,



Joyce T. Willoughby
Inspector General



EXECUTIVE SUMMARY

This Semiannual Report summarizes the Office of Inspector General's activities and accomplishments from April 1, 2024, to September 30, 2024. The Office of Inspector General issued one audit report and two evaluation reports. The Office of Inspector General received 72 hotline contacts during the reporting period.

Completed and ongoing activities include the following:

Completed Audit Activity

- 2024 Inspector General Cyberscope reporting metrics for the Equal Employment Opportunity Commission

Ongoing Audit Activities

- An audit regarding compliance with the Federal Information Security Modernization Act of 2014 for FY 2024
- An audit of the Agency's financial statements for FY 2024

Completed Other Audit Activities

- A peer review of the Denali Commission
- A peer review of the Commodity Futures Trading Commission
- A review of the Agency's compliance with the Federal Managers' Financial Integrity Act of 1982 and the Office of Management and Budget Circular A-123 for FY 2024

Completed Evaluation Activities

- An evaluation of EEOC's fair employment practice agencies
- A review of EEOC's compliance with the payment integrity

Ongoing Evaluation Activities

- An evaluation regarding Agency data reliability and governance
- An evaluation of the Agency's tribal program
- A review regarding FY 2025 Agency management challenges

Completed Other Evaluation Activities

- A peer review of the Library of Congress, Office of Inspector General

Ongoing Other Special Projects

- An information request regarding Agency Anti-Gag provisions
- An inquiry regarding political bias against EEOC employees



Completed Investigative Activities

- An investigation regarding an employee using government resources for personal use
- An investigation regarding a charging party uploading possible child pornography into an Agency system
- An investigation that an Agency employee had a financial conflict of interest

Ongoing Investigative Activities

- Alleged false filing of a workman's compensation claim
- Alleged disclosure of privileged information and misuse of position by EEOC officials



INTRODUCTION

The Equal Employment Opportunity Commission

The US Equal Employment Opportunity Commission (EEOC) is responsible for enforcing federal laws that make it illegal to discriminate against a job applicant or an employee because of the person's race, color, religion, sex (including pregnancy, childbirth, or related conditions, gender identity, and sexual orientation), national origin, age (40 or older), disability or genetic information.

The EEOC is a bipartisan commission comprised of five presidentially appointed members, including the Chair, Vice-Chair, and three Commissioners. The Chair is responsible for administering and implementing policy and the Commission's financial management and organizational development of the Commission. The Vice-Chair and the Commissioners participate equally in developing and approving Commission policies, issue charges of discrimination where appropriate, and authorize the filing of lawsuits. In addition to the Commissioners, the President of the United States appoints a General Counsel to support the Commission and provide direction, coordination, and supervision to the EEOC's litigation program.

The EEOC Office of Inspector General

The US Congress established an Office of Inspector General at the EEOC through the 1988 amendment of the Inspector General Act of 1978. The Office of Inspector General supports the Agency by conducting audits, investigations, and program evaluations intended to prevent and detect fraud, waste, and abuse.

The Office of Inspector General is under the leadership of the Inspector General, who provides overall direction, coordination, and supervision to staff. In the EEOC, a designated federal entity, the Inspector General is appointed by and is under the general supervision of the Commission Chair. Even so, the Inspector General has a dual role since they also report directly to Congress. The EEOC leadership cannot prevent the Office of Inspector General from conducting an audit, investigation, or other work. The Office of Inspector General includes a deputy inspector general, auditors, evaluators, investigators, chief technology officer, information technology specialist, independent counsel, and administrative staff.

Finally, during the first quarter of FY 2025, the Office of Inspector General is required to report in the EEOC's Agency Financial Report what it has determined to be the most serious management and performance challenges facing the Agency. This statement provides our views on the Agency's fiscal year (FY) 2025 challenges. We plan to issue our management challenges report before October 16, 2024 (please visit <https://oig.eeoc.gov> to read our Management Challenges report).



THE AUDIT PROGRAM

The Audit Program supports the Office of Inspector General's mission by conducting reviews that improve the Agency's economy, efficiency, and effectiveness regarding EEOC programs, operations, and activities.

Completed Other Audit Activity

Issuance of Inspector General (IG) Federal Information Security Modernization Act (FISMA) FY 2024 Cyberscope Reporting Metrics for the Equal Employment Opportunity Commission.

On July 26, 2024, the Office of Inspector General issued its FY 2024 Inspector General, Federal Information Security Modernization Act Cyberscope reporting metrics review. The Office of Inspector General contracted with Harper, Rains, Knight & Company, PA to complete our metrics review.

Harper, Rains, Knight & Company, PA found EEOC's information security program effective.

Ongoing Audit Activities

Audit of the EEOC's FY 2024 Financial Statements

The Office of Inspector General has contracted with the public accounting firm Harper, Rains, Knight & Company, PA to audit the EEOC's financial statements for FY 2024 and 2023 as required by the Accountability of Tax Dollars Act of 2002. Harper, Rains, Knight & Company, PA will examine the Agency's financial statements and accompanying disclosures.

The OIG will issue the final report no later than November 15, 2024.

Audit of the EEOC's Compliance with Provisions of the Federal Information Security Modernization Act (FISMA) of 2014.

The Office of Inspector General has contracted with Harper, Rains, Knight & Company, PA to perform an independent audit of the Equal Employment Opportunity Commission's information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA).

Our office will issue the final report no later than the first quarter of FY 2025.



Completed Other Audit Activities

Peer Review of the Denali Commission, Office of Inspector General

On May 10, 2024, the Office of Inspector General completed a peer review of the audit function of the Denali Commission, Office of Inspector General.

Our office determined that the Denali OIG had controls in-place to ensure that the Independent Public Accountants (IPA) performed contracted work in accordance with professional standards.

Peer Review of the Commodity Futures Trading Commission, Office of Inspector General

On May 31, 2024, the Office of Inspector General completed a peer review of the Commodity Futures Trading Commission, Office of Inspector General audit function.

Our office determined that the system of quality control was not suitably designed and complied with to provide reasonable assurance of performing and reporting in conformity in all material respects with applicable professional standards and applicable legal and regulatory requirements.

Other Ongoing Audit Activities

EEOC's Compliance with the Federal Managers' Financial Integrity Act of 1982 for FY 2024

The Office of Inspector General is reviewing the Agency's compliance with the Federal Managers' Financial Integrity Act of 1982 for FY 2024. Our office will issue an independent report describing whether the Agency's management control review was conducted in accordance with applicable EEOC Order 195.001, federal law, and applicable Office of Management and Budget guidance.

The OIG will issue its report no later than the first quarter of FY 2025.



The Evaluation Program

The Evaluation Program supports the Office of Inspector General's missions by executing ambitious, high-value evaluations and special assessments. Evaluations analyze the management, effectiveness, and efficiency of programs that have the most significant effect on mission accomplishment.

Completed Evaluation Activities

Evaluation of Fair Employment Practice Agencies (FEPA) Program

On August 19, 2024, the Office of Inspector General completed an evaluation of the Agency's fair employment practice agencies. Our office contracted with Clarus Research to evaluate the EEOC's fair employment practices agencies management activities. The primary purpose of the evaluation was to provide EEOC's leadership and stakeholders with data, analysis, and recommendations to improve the effectiveness and efficiency of key FEPA program activities.

Clarus Research's report contained recommendations that highlighted cross-cutting themes demonstrating to the need for the EEOC to clarify and develop processes, plan and provide training, solicit input from FEPAs, and communicate clearly and consistently with FEPAs.

US Equal Employment Opportunity Commission Payment Integrity Information Act of 2019 (PIIA) for FY 2023

On May 29, 2024, the Office of Inspector General issued its review of the EEOC's compliance with the Payment Integrity Information Act of 2019 for FY 2023. The Office of Inspector General contracted with the certified public accounting firm of Harper, Rains, Knight & Company, PA to conduct the evaluation. Harper, Rains, Knight & Company, PA determined EEOC was not compliant with PIIA annual reporting consistent with Appendix C of OMB Circulars A-123 and A-136.

Ongoing Evaluation Activities

EEOC Data Governance Assessment

The Office of Inspector General is evaluating EEOC's Data Governance and reliability. This project will assess EEOC's management of data accuracy, completeness, and reliability for EEOC's ARC and data warehouse.

Evaluation of EEOC's Tribal Program

The Office of Inspector General plans to conduct an evaluation of EEOC's management of the Tribal Program to assess the strategic management of key program activities.



Completed Other Evaluation Activities

Peer Review of the Library of Congress. Office of Inspector General

On August 16, 2024, the Office of Inspector General issued a peer review report of the Library of Congress, Office of Inspector General evaluation program.

In our opinion, the system of quality control for the Library of Congress, Office of Inspector General evaluation program in effect for the year ended March 31, 2024, has been suitably designed and complied with the Council of Inspectors General for Integrity and Efficiency Blue Book standards.

OTHER SPECIAL PROJECTS

Special Projects are often one-time projects (e.g., management advisories, congressional inquiries) that may or may not be performed using Government Auditing Standards or CIGIE Quality Standards for Inspection and Evaluation.

Ongoing Special Projects Activity

US Equal Employment Opportunity Commission, Office of Inspector General Response to Senator Charles E. Grassley's Request Regarding EEOC Implementation of Federal Anti-Gag Regulations

On March 11, 2024, the Office of Inspector General received a request from Senator Charles Grassley's office to review all nondisclosure policies, forms, agreements, and related documents specific to the US Equal Employment Opportunity Commission to ensure the anti-gag provision is included as required by law. Our office will respond to Senator Grassley's request during the first quarter of FY 2025.

Review of Employee Bias Based on Political Affiliation

The Office of Inspector General is conducting an inquiry regarding concerns raised by several Commission employees or members that certain EEOC officials were showing bias against other EEOC employees based on political affiliation.



AUDIT AND EVALUATION FOLLOW - UP

Audit and Evaluation Follow-up is an integral part of effective management. It is a shared responsibility of agency management officials, auditors, and evaluators. Corrective action taken by management to resolve findings and recommendations is essential to improving agency operations, effectiveness, and efficiency.

Audit and Evaluation Reports Issued During This Reporting Period

Section 5(a)(1) of the Inspector General Act of 1978, as amended, requires that semiannual reports include a summary description of significant problems, abuses, and deficiencies relating to the Agency's administration of programs and operations disclosed by the Office of Inspector General during the reporting period. The Office of Inspector General issued **two** evaluation reports with **ten** recommendations.

Fiscal Year	Report Number	Report Title	Date Issued	Number of Recommendations
2024	2024-001-EOIG	US Equal Employment Opportunity Commission Payment Integrity Information Act of 2019 (PIIA) for FY 2023	5/29/2024	2
2024	2023-003--EOIG	Evaluation of Fair Employment Practice Agencies (FEPA) Program	8/19/2024	8

Recommendations for Which Corrective Actions Have Not Been Completed

As required by Section 5(a)(3) of the Inspector General Act of 1978, as amended, semiannual reports shall provide an identification of each significant recommendation described in previous semiannual reports for which corrective action has not been completed.

The Office of Inspector General reports audit and evaluation reports with open recommendations for this reporting period. The Office of Inspector General reports audit reports with open recommendations and evaluation reports with open recommendations. The following table shows those recommendations for which corrective actions have not been completed. There are **fifteen** Office of Inspector General reports and with **fifty** open recommendations.



Fiscal Year	Report Number	Report Name	Date Issued
2024	2023-001-AOIG	Audit of the EEOC FY 2023 and 2022 Financial Statements	11/15/2024
<p>1. We recommend that EEOC adjust the balances for all activity as of September 30, 2023, and vigilantly monitor transactions related to software under development, especially those associated with the TMF. As such, OIT should notify OCFO at least quarterly of all activity related to software under development for proper recording of costs associated with internally developed software.</p> <p>2. We recommend EEOC review all State and Local Program undelivered orders at year end and accrue an estimated value of these payments that will be made after year-end. As the State and Local Program is a reimbursement for the current year activity, the expectation is that a significant amount of these transactions will be submitted for reimbursement. EEOC should perform a historical review of State and Local Program reimbursements against contracts to determine an estimate to apply to all unpaid State and Local Program undelivered orders at each year end. Utilizing this historical ratio against current year outstanding undelivered orders as an accrual amount should help ensure that EEOC capture its costs for the fiscal year.</p>			

Fiscal Year	Report Number	Report Name	Date Issued
2024	2023-002-AOIG	FY 2023 Federal Information Security Modernization Act Independent Evaluation	11/20/2023
<p>1. We recommend that EEOC communicates and implements an organization-wide SCRM and C-SCRM strategy to guide supply chain analyses, provide communication channels with internal/external partners and stakeholders, and assist in building consensus regarding the appropriate resources for SCRM and C-SCRM. We recommend that EEOC offices of the Chief Financial Officer and the Chief Information Officer identify SCRM/C-SCRM as a risk to be included in their respective ERM risk registers until the issue is resolved so that commission management understand that SCRM/C-SCRM is a commission-wide requirement.</p> <p>2. We recommend that EEOC continue its full implementation in accordance with their plan. For the ZTA Identity pillar, to better meet ZT requirements for all agency-provided devices, the EEOC made a strategic decision to move away from the prior PIV-based device-login solution to a new password-less Multifactor Authentication</p>			



(MFA) strategy - providing a strong, non-impersonable authentication process for all agency resource access.

3. We recommend that EEOC plans and prepares to meet the goals of the TIC initiative, consistent with OMB M-19-26. The Agency should define and customize, as appropriate, a set of policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays.

4. EEOC should develop an executable plan to meet the requirements of OMB M-21-31 and ensure the plan is properly supported.

5. We recommend that EEOC's information security team should, in conjunction with other EEOC offices: a. Identify and document all applicable policies and procedures to cybersecurity and information security; b. Develop and use an accessible repository, such as SharePoint, for all identified documents, regardless of what office they reside in; c. Design a risk-based approach to review and update all identified documents in the repository, including who is responsible for reviewing and updating each document. d. Document the review/update in each document, as well as the responsible party within the information security team who ensures that each document has been updated per the documented procedure for review. e. Designate a responsible official within the OIT to review and update the process as necessary on an annual basis.

6. We recommend that EEOC: • Review all devices and systems and ensure default credentials are not in use. • Implement the use of complex credentials for all systems. • We recommend that EEOC review system for potential malicious access. • If it is not possible to change passwords to something complex, consider isolating the device on a separate network segment and implementing ACLs that limit what devices and who may attach to the system. • Determine if the application should be publicly available. If not, implement NSG rules within Microsoft Azure or ACLs within firewalls to limit or block all external applications to the site. • Ensure it has a policy in place that addresses NIST 800-53, Rev 5, IA-5(5). • Ensure procedures are written in such a way to accomplish what is written in the policy. • Ensure it has people in assigned a role to follow and evaluate default credentials. • Consider how new or existing technologies it has can assist in these efforts.

7. We recommend that EEOC: • Update to a recent BIRT viewer component, well past version 4.12. • Determine if the application should be publicly available. If not, implement NSG rules within Microsoft Azure or ACLs within firewalls to limit or block all external applications to the site. • Remove default and un-needed .rptdesign files that allow for passing a parameter with attacker controlled input. • Ensure BIRT viewer component is proxied through an authenticated connection and not via direct calls to the NXG servers. Implement the use of complex credentials for all systems. • Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2. • Ensure procedures are



written in such a way to accomplish what is written in the policy. • Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance. • Consider how new or existing technologies it has can assist in these efforts.

8. We recommend that EEOC: • Review all devices and systems and ensure default credentials are not in use. • Implement the use of complex credentials for all systems. • It is not possible to change this password to something complex. Consider isolating the device on a separate network segment and implementing ACLs that limit what devices and who may attach to the system. • Determine if the management page should be publicly available. If not, implement ACLs within firewalls to limit or block all external application to the site.

• Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2. • Ensure procedures are written in such a way to accomplish what is written in the policy. • Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance. • Consider how new or existing technologies it has can assist in these efforts.

9. We recommend that EEOC: • Patch to the most recent version of firmware and confirm that this information is not disclosed from the administrative page source code. • Determine if the management page should be publicly available. If not, implement ACLs within firewalls to limit or block all external application to the site. • Ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2. • Ensure procedures are written in such a way to accomplish what is written in the policy. • Ensure it has people in assigned a role to remediate flaws in accordance with its policy and risk tolerance. • Consider how new or existing technologies it has can assist in these efforts...

10. We recommend that EEOC: • Review source code and source code repositories for code containing internal IP addresses and URLs. • Remove inappropriately stored information from source code.

11. We recommend that EEOC: • Limit access from specific IP addresses to the Amazon AWS EKS API. • Configure AWS Control Tower's data residency controls to alert on publicly accessible Amazon EKS endpoints. • If AWS Control Tower is not in use, create an AWS Config rule to detect whether an Amazon EKS endpoint is blocked from public access.

12. We recommend that EEOC ensures that every sensitive form transmits content over HTTPS. • Ensure it has a policy in place that addresses and, enforces protects the confidentiality and the integrity of transmitted information. • Ensure procedures are written in such a way to accomplish what is written in the policy, to include compensating controls. • Ensure it has people in assigned a role to enforce the policy and procedures in place to protect the confidentiality and/or the integrity of transmitted information. Consider how new or existing technologies it has can assist in these efforts....

13. We recommend that the EEOC ensure it has a policy in place to address NIST 800-53, Rev 5, SI-2, Flaw Remediation. • Ensure procedures are written in such a way to accomplish what is written in the policy.

Fiscal Year	Report Number	Report Name	Date Issued
2022	2022-001-AOIG	FY 2022 Federal Information Security Modernization Act Independent Evaluation	11/3/2022

1. We recommend that EEOC defines, communicates, and implements an organization-wide SCRM strategy to guide supply chain analyses, provide communication channels with internal/external partners and stakeholders, and assist in building consensus regarding the appropriate resources for SCRM.
2. We recommend that EEOC implement strong authentication mechanisms for privileged and non-privileged users in accordance with Federal guidance, to meet the required use of PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) credential of the Agency's networks, including remote access sessions, in accordance with Federal targets. The Agency should continue developing their plans for organization-wide use of strong authentication mechanisms for non-privileged users and require multifactor authentication to network access for all user accounts.
3. We recommend that EEOC review and remediate the medium level severity vulnerabilities identified during external penetration testing by:
 - Disabling IKE Aggressive Mode if supported;
 - Refraining from the use of pre-shared authentication keys;
 - If using a pre-shared key cannot be avoided, use strong keys;
 - Do not allow VPN connections from non-approved IP addresses, if possible.
4. We recommend that EEOC:
 - Determine if listening ports or entire system should be blocked from public access;
 - Regularly review network device search engines for new systems belonging to EEOC or those that may be masquerading as EEOC systems;
 - Perform a forensic analysis on identified system to ensure no malicious access has taken place;
 - For authorized remote sessions, create a control to address remote access being left open after the session has concluded. The controls should, at minimum, require the session owner to ensure the remote session was closed at the conclusion of the session as well as an overall control run on a set basis that will identify any open remote sessions on endpoints;



- Create an auditability feature that checks internally via an agent when a device with remote access is listening;
- Create an auditability feature that checks for remote connection software;
- 5. We recommend that EEOC review and remediate the level 4 severity vulnerabilities identified during internal vulnerability scanning to avoid compromises to agency systems. (See Attachment B for the full list of vulnerabilities identified, including those identified as Level 4.);
 - To remediate vulnerabilities and prevent further exploitation, the Agency should implement risk mitigation procedures such as: performing system updates, operating systems with administrative rights, downloading patches, uninstalling unprotected applications, etc;
 - Where risk acceptance is required for vulnerabilities based on EEOC's network operations and risk assessments, we recommend that EEOC formally document the risk acceptance along with any associated mitigation activities;
- 6. We recommend that EEOC review and remediate the level 5 severity vulnerabilities identified during internal vulnerability scanning to avoid compromises to agency systems. (See Attachment B for the full list of vulnerabilities identified, including those identified as Level 5.);
 - To remediate vulnerabilities and prevent further exploitation, the Agency should implement certain user access rights, upgrading to the latest supported version, and removing vulnerable/obsolete hardware from its network.
 - These vulnerabilities should be added and tracked on POAMS.
 - Where risk acceptance is required for vulnerabilities based on EEOC's network operations and risk assessments, we recommend that EEOC formally document the risk acceptance along with any associated mitigation activities.

Fiscal Year	Report Number	Report Name	Date Issued
2022	2021-004-AOIG	Performance Audit Report US Equal Employment Opportunity Commission Federal Information Security Modernization Act of 2014 (FISMA)	3/15/2022

1. We recommend that EEOC plans and prepares to meet the goals of the TIC initiative, consistent with OMB M-19-26. The Agency should define and customize, as appropriate, a set of policies, procedures, and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB



M-19-26. This includes, as appropriate, incorporation of TIC security capabilities catalog, TIC use cases, and TIC overlays.

2. We recommend that EEOC review and remediate the medium-level severity vulnerabilities identified during external penetration testing by: (1) Disabling IKE Aggressive Mode. (2) Refraining from the use of pre-shared authentication keys. (3) Implementing multifactor authentication for all VPN access.

Fiscal Year	Report Number	Report Name	Date Issued
2021	2020-004-AOIG	Performance Audit of the EEOC Commercial Charge Card Program	3/24/2021
<ol style="list-style-type: none"> 1. We recommend EEOC ensure that emailed policy memos are promptly updated in the appropriate EEOC Directives Transmittal Order. 2. For purchase cards, EEOC management should create a control where management reviews, on a sample basis, purchase cards transactions to ensure all obligating documents and purchase orders are in conformity with EEOC Directives Transmittal Order 360.003, Commercial Purchase Charge Card Program Practical User's Guide. For travel cards, EEOC management should create a control where management reviews, on a sample basis, travel card transactions to ensure all travel authorization or vouchers and receipts are in conformity with EEOC Directives Transmittal Order 345.001, Travel and Transportation Administrative Policies and Procedures Manual. 3. We recommend EEOC management update its policies and procedures to include all required safeguards and internal controls to be compliant with the Government Charge Card Abuse Prevention Act of 2012. In addition, EEOC should create a monitoring control to review the policy when changes or updates are made to federal law or Office of Management and Budget or General Services Administration guidance. 			

Fiscal Year	Report Number	Report Name	Date Issued
2021	2020-002-AOIG	Management Letter - FY 2020 Financial Statement Audit	12/16/2020
<ol style="list-style-type: none"> 1. We recommend EEOC management create a control where management reviews, on a sample basis, at least quarterly, the approved PP&E disposals/retirements for conformity to EEOC SOP for OIT Excess Property that states, "When equipment is disposed of, an SF 120, SF 122, or SF 120 copy using GSAXcess, is approved by the EEOC Approving Official, CSD Backup or Property manager, evidenced by their signature and date." EEOC management should follow-up with Approving Official(s), 			



CSD Backup or Property management who have been found to not adhere to requirements of the SOPs for OIT Excess Property and require them to obtain additional training, to include certifying they have read the Approving Officials responsibilities, as it relates to the aforementioned control. **(Repeat Finding)**

Fiscal Year	Report Number	Report Name	Date Issued
2019	2018-007-AOIG	FY 2017 and FY 2018 Performance Audit of the US Equal Employment Opportunity Commission Commercial Charge Card Program	5/31/2019

1. We recommend that the Office of the Chief Financial Officer of the US Equal Employment Opportunity Commission enhance the documentation, monitoring, and enforcement of its controls over the closure of charge card accounts.
 - For purchase cards, the Administrative Officer (AO) or District Resources Manager (DRM) should maintain documentation of all account closures electronically or in hard copy. Documentation should include evidence of the name of the AO or DRM who received the employee's charge card, the date the card was turned in, the date the card was physically destroyed, and the date that account closure was confirmed by the Charge Card Vendor. The policy or procedure should include monitoring by the Agency/Organization Program Coordinator (A/OPC) and/or Agency Alternative/Organization Program Coordinator (AA/OPC) and appropriate disciplinary actions for noncompliance.
 - For travel cards, the Charge Card Program Manager (CCPM) should maintain documentation of all account closures electronically or in hard copy. Documentation should include evidence of the name of the immediate supervisor and/or servicing personnel officer who received the employee's charge card, the date the card was turned in, the date the card was cut in half, and the date that account closure was confirmed by the Charge Card Vendor. The policy or procedure should include monitoring by the CCPM and appropriate disciplinary actions for noncompliance. **(Repeat Finding)**

EVALUATION OPEN RECOMMENDATIONS

Fiscal Year	Report Number	Report Name	Date Issued
2023	2023-001-EOIG	Independent Evaluation of US Equal Employment Opportunity Commission's Compliance with the Payment Integrity Information Act of 2019 for FY 2022	5/22/2023
<ol style="list-style-type: none"> 1. We recommend that EEOC develops a SOP to ensure annual compliance with OMB A-136 PIIA review and reporting requirements. 2. We recommend that EEOC develops agency-wide Improper Payment risk assessment standard operating procedures (SOP). This SOP should include risk assessment procedures to be performed by each identified significant program. These procedures should be based on OMB A-123 guidance found in Appendix C. For each identified significant program, a responsible program point of contact should be established. The responsible party should report results of their programs risk assessment to the EEOC responsible official (or office). 			

Fiscal Year	Report Number	Report Name	Date Issued
2022	2022-001-IOIG	FY 2021 Annual Report on EEOC's Compliance with the Payment Integrity Information Act of 2019 (PIIA)	7/11/2022
<ol style="list-style-type: none"> 1. We recommend that EEOC should conduct an annual improper payment review in accordance with PIIA and follow the guidance outlined in OMB Circular A-136, section II.4.5 [Payment Integrity Information Act Reporting]. 2. We recommend that EEOC should report the OIG's finding of non-compliance with the FY 2021 PIIA requirements, as outlined in OMB Memorandum M-21-19, Section VI.D, "Agency Responsibility When a Program is Non-Compliant." 			



Fiscal Year	Report Number	Report Name	Date Issued
2023	2021-002-EOIG	Digital Process Transformation and Automation Evaluation	1/20/2023
<ol style="list-style-type: none"> 1. Define a clear, consistent, and comprehensive vision of digital transformation at EEOC. 2. Consider formulating a Digital Transformation Strategy, either as a strategic goal in the EEOC Strategic Plan for Fiscal Years 2023 – 2027 or as a standalone document. 3. Plan at least three digital pilot projects with appropriate evaluation methods. 4. Task OEDA with a goal of building a Data Analytics Plan for EEOC. 5. Develop an EEOC Organizational Communication Strategy and Plan. 6. Develop a Target-State Architecture Plan. 7. Inventory and plan the decommissioning of outdated technologies and online content. 			

Fiscal Year	Report Number	Report Name	Date Issued
2023	2022-001-EOIG	Customer Service Portals Evaluation	9/12/2023
<ol style="list-style-type: none"> 1. Include requirements to use the US Web Design System in the Agency's Project Plan for designing, developing, and implementing the next generation of portals. 2. Implement mechanisms to ensure that the design and management of the portals are responsive to customer needs. 3. Ensure that the design and function of all portals accurately reflect EEOC's business rules and applicable laws. 4. Make targeted improvements to address accessibility issues on the existing portals. 			



Fiscal Year	Report Number	Report Name	Date Issued
2023	2021-001-EOIG	Evaluation of EEOC's Management of Private Sector Customer Service Program	10/18/2022
<ol style="list-style-type: none"> 1. EEOC should develop a customer service plan to include establishing goals and objectives, developing performance metrics that target the goals, and measuring performance against the goals. This plan must include goals and metrics for the IIG. 2. EEOC must manage customer expectations by making customer service standards available to the public. 			

Fiscal Year	Report Number	Report Name	Date Issued
2021	2020-001-EOIG	Evaluation of EEOC's Social Media Program	7/26/2021
<ol style="list-style-type: none"> 1. Implement a consistent content approval process run by OCLA. 2. Complete revisions to the social media handbook and provide to all staff managing social media channels. 			

Fiscal Year	Report Number	Report Name	Date Issued
2020	2019-001-EOIG	Evaluation of EEOC's Contract Administration Activities	11/19/2019
<ol style="list-style-type: none"> 1. OCFO should revise EEOC Order 360.001 as needed to assist in performing their duties. Include implementation guidance for contract administrative activities such as submitting contract modifications. 			



Fiscal Year	Report Number	Report Name	Date Issued
2020	2018-001-EOIG	Evaluation of EEOC's Federal Hearings and Appeals Processes	3/27/2020
<ol style="list-style-type: none"> 1. OIT developers should meet directly with software users, such as OFO attorneys and supervisory attorneys and OFP AJs and Supervisory AJs (SAJ) to determine additional requirements. 2. Assign a target amount of days for intake so that management can determine if changes implemented impact the efficiency of the process. 			

Audit and Evaluation Reports Which no Management Decision has been Made by the End of the Reporting Period

The Office of Inspector General has no audit or evaluation reports issued before the reporting period began, for which no management decision was made.

Fiscal Year	Number of Reports with Unimplemented Recommendations (such as report title, report number, hyperlink to report, etc.)	Number of Unimplemented Recommendations	Dollar Value of Aggregate Potential Cost Savings	For which no establishment comment was returned within 60 days of providing the report to the establishment
2024	0	0	0	N/A

THE INVESTIGATION PROGRAM

The Investigation Program supports the Office of Inspector General's strategic goal by focusing its limited investigative resources on issues that represent the most significant risk and offer the maximum opportunity to detect and prevent fraud, waste, and abuse in EEOC programs and operations.

The Office of Inspector General received 72 investigative contacts from April 1, 2024, through September 30, 2024, resulting in the following:

Investigative Inquiries Received April 1, 2024, through September 30, 2024	
Allegations	Number
Charge Processing	30
Ethics Violations	15
Theft	1
Fraud	3
Mismanagement	13
Other Criminal Allegations	5
Threats	1
Other Statutes	4
Total	72

Office of Inspector General Hotline

The Office of Inspector General Hotline is a clearinghouse for receiving and handling allegations regarding fraud, waste, abuse, mismanagement, or misconduct affecting Equal Employment Opportunity Commission programs and operations. Examples of allegations that should be reported to the hotline include misuse, embezzlement, or theft of government property or funds; contract or procurement fraud; contractor misconduct; employee misconduct, such as misuse of official position; bribes or unauthorized acceptance of gifts; conflicts of interest, and other ethical violations.

Some complaints received by the Office of Inspector General are outside its jurisdiction. The Office of Inspector General frequently receives reports and allegations of misdirected complaints/inquiries belonging to other EEOC offices, federal agencies, law enforcement agencies, or other state or local government entities. Reviewing and responding to these reports and allegations can entail significant staff time and effort. In these instances, Office of Inspector General personnel strive to provide excellent customer service and offer the complainant the appropriate contact information to the entity that may address their needs. The complaint/inquiry may be redirected and sent directly from the Office of Inspector General to the appropriate office or Agency.

Closed Investigative Activities

The OIG has closed the following investigative activities:

- An investigation regarding an employee use of government resources for personal use
- An investigation regarding a charging party uploading possible child pornography into an Agency system
- An investigation that an Agency employee may have had a financial conflict of interest

Ongoing Investigative Activities

The OIG has ongoing investigations in several field offices involving the following:

- Alleged false filing of a workman's compensation claim
- Alleged disclosure of privileged information and misuse of position by EEOC officials



APPENDICES

Appendix I. Final Audit/Evaluation/Inspection Reports

Report Title	Date Issued	Questioned Costs	Funds Put to Better Use	Unsupported Costs
Evaluation of Fair Employment Practice Agencies (FEPA) Program	August 19, 2024	-0-	-0-	-0-
US Equal Employment Opportunity Commission Payment Integrity Information Act of 2019 for FY 2023	May 29, 2023	-0-	-0-	-0-

Appendix II. Investigative Statistical Report

Report Title	Number
Total number of investigative reports	-0-
Total number of persons referred to the Department of Justice for criminal prosecution during the reporting period	-0-
Total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period	-0-
Total number of indictments and criminal information during the reporting period that resulted from any prior referral to prosecuting authorities	-0-

Appendix III. A Report on Each Investigation Conducted by the Office Involving a Senior Government Employee Where Allegations of Misconduct Were Substantiated.

Report Name: N/A Report Number: N/A Date Issued N/A

Facts and circumstances of the investigation	(B) the status and disposition of the matter, including- (i) if the matter was referred to the Department of Justice, the date of the referral; and (ii) if the Department of Justice declined the referral, the date of the declination
No	N/A

Appendix IV. A Detailed Description of Any Instance of Whistleblower Retaliation.

Information about an official found to have engaged in retaliation.	Consequences the establishment imposed to hold that official accountable.
No	N/A

Appendix V. A Detailed Description of Any Attempt by the Establishment to Interfere with the Independence of the Office of Inspector General.

Issue	Description
With budget constraints designed to limit the capabilities of the office	No
Incidents where the establishment has resisted or objected to oversight activities of the office or restricted or significantly delayed access to information, including the justification of the establishment for such action	No



Appendix VI. Detailed Descriptions of the Particular Circumstances.

Issue	Description
Inspection, evaluation, and audit conducted by the office that is closed and was not disclosed to the public	No
An Investigation conducted by the office involving a senior Government employee that is closed and was not disclosed to the public	No

Appendix VII. Significant Management Decision (s)

Issue	Description
Significant Management Decisions That Were Revised During the Reporting Period	N/A
Significant Management Decisions with which the Office of Inspector General is in disagreement	N/A

Appendix VIII. Index of Reporting Requirements

Inspector General Act Citation	Reporting Requirements	Page
Section 4(a)(2)	Review of Legislation and Regulations	N/A
Section 5(a)(1)	Significant Problems, Abuses, and Deficiencies	N/A
Section 5(a)(2)	Recommendations with Respect to Significant Problems, Abuses, and Deficiencies	N/A
Section 5(a)(3)	Significant Recommendations Included in Previous Reports on Which Corrective Action Has Not Been Completed	11-22
Section 5(a)(4)	Matters Referred to Prosecutorial Authorities	26
Section 5(a)(5)	Summary of Instances Where Information Was Refused	27
Section 5(a)(6)	List of Reports	26
Section 5(a)(7)	Summary of Significant Reports	7-10
Section 5(a)(8)	Questioned and Unsupported Costs	26
Section 5(a)(9)	Recommendations That Funds Be Put to Better Use	26
Section 5(a)(10)	<p>Summary of each audit report, inspection, and evaluation report(s) issued before the commencement of the reporting period:</p> <p>(A) for which no management decision has been made by the end of the reporting period (including the date and title of each such report), an explanation of the reasons such management decision has not been made, and a statement</p>	23



	<p>concerning the desired timetable for achieving a management decision on each such report;</p> <p>(B) for which no establishment comment was returned within 60 days of providing the report to the establishment; and</p> <p>(C) for which there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.</p>	
Section 5(a)(11)	Significant Management Decisions That Were Revised During the Reporting Period	28
Section 5(a)(12)	Significant Management Decisions with Which the Office of Inspector General is in disagreement	28
Section 5(a)(17)	<p>Statistical tables showing:</p> <p>(A) the total number of investigative reports issued during the reporting period;</p> <p>(B) the total number of persons referred to the Department of Justice for criminal prosecution during the reporting period;</p> <p>(C) the total number of persons referred to State and local prosecuting authorities for criminal prosecution during the reporting period; and</p> <p>(D) the total number of indictments and criminal information during the reporting period that resulted from any prior referral to prosecuting authorities.</p>	26

Section 5(a)(19)	<p>A report on each investigation conducted by the office involving a senior Government employee where allegations of misconduct were substantiated, including a detailed description of:</p> <p>(A) the facts and circumstances of the investigation; and</p> <p>(B) the status and disposition of the matter, including:</p> <p>(i) if the matter was referred to the Department of Justice, the date of the referral; and</p> <p>(ii) if the Department of Justice declined the referral, the date of the declination.</p>	27
Section 5(a)(20)	<p>A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation and what, if any, consequences the establishment imposed to hold that official accountable.</p>	27
Section 5(a)(21)	<p>A detailed description of any attempt by the establishment to interfere with the independence of the office, including:</p> <p>(A) with budget constraints designed to limit the capabilities of the office; and</p> <p>(B) incidents where the establishment has resisted or objected to oversight activities of the office or restricted or significantly delayed access to information, including the justification of the establishment for such action.</p>	27
Section 5(a)(22)	<p>Detailed descriptions of the particular circumstances of each:</p> <p>(A) inspection, evaluation, and audit conducted by the office that is closed and was not disclosed to the public; and</p> <p>(B) an investigation conducted by the office involving a senior Government employee that is closed and was not disclosed to the public.</p>	28

Appendix IX. Single Audit Act Reporting

The Single Audit Act of 1984 established requirements for audits of states, local governments, and Indian tribal governments that administer federal financial assistance programs. Independent non-Federal auditors, such as public auditing firms and State auditors, conduct Single Audits.

During the reporting period, the OIG received no audit reports from independent auditors concerning Fair Employment Practice Agencies with work-sharing agreements with the EEOC.

Appendix X. Peer Review Reporting

As required by the Government Auditing Standards and the Quality Standards for Inspection and Evaluation, The Office of Inspector General Audit and Evaluation programs must have an external peer review of its quality control system.

On November 6, 2023, the Federal Maritime Commission, Office of Inspector General, issued its peer review report on our Audit program to determine if established policies and procedures were current and consistent with applicable professional standards. Based on its review, the established policies and procedures for the Equal Employment Opportunity Commission, Office of Inspector General audit function at March 31, 2023, were current and consistent with applicable professional standards as stated.

On March 15, 2023, the Pension Benefit Guaranty Corporation, Office of Inspector General, issued its modified peer review report on our Evaluation program. The review team determined that the Office of Inspector General evaluation section policies and procedures generally were consistent with the Blue Book standards addressed in the external peer review. Of the three reports reviewed, all of them generally complied with the Blue Book standards.



Contact Us

The Office of Inspector General is at the forefront of the Nation's efforts to fight waste, fraud and abuse in EEOC programs and operations. If your question refers to programs that are not part of EEOC you can find contacts for all Federal agencies on the USA.gov website's <https://www.usa.gov/federal-agencies>



For general inquiries, please visit:

<https://oig.eeoc.gov/contact>

To electronically report fraud, waste, abuse, and potential wrong-doing please visit:

<https://oig.eeoc.gov/hotline>



Toll-free Number:

1-800-840-3237

Fax Number

202-221-7781



For written inquiries, please send mail to:

Office of Inspector General

Equal Employment Opportunity Commission

131 M. St. Suite 6NE23M

Washington, DC 20507



Contact Us QR code



EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

OFFICE OF INSPECTOR GENERAL

Your identity when contacting the OIG is fully protected and confidential