U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Performance Audit of the Agency's Personnel Security Program
OIG REPORT NUMBER 2013-08-PSA

September 15, 2014

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
PERFORMANCE AUDIT OF THE AGENCY'S
PERSONNEL SECURITY PROGRAM

Table of Contents

September 15, 2014

Milton A. Mayo Jr.
Inspector General
Equal Employment Opportunity Commission

Dear Mr. Mayo,

Williams, Adley & Company-DC, LLP performed a performance audit of the U.S. Equal Employment Opportunity Commission's (EEOC) Personnel Security Program for calendar year 2013. The audit was performed in accordance with our Task Order No. EECIGA-UD-0-07, dated September 26, 2013. This report presents the results of the audit, and includes recommendations to help improve efficiency and effectiveness of EEOC's Personnel Security Program.

Our audit was conducted in accordance with applicable *Government Auditing Standards*, 2011 revision. The audit was a performance audit, as defined by Chapter 2 of the *Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the opportunity to have conducted this audit. Should you have any questions or need further assistance, please contact Charbet Duckett, Partner at (202) 371-1397.

Sincerely,

Charbet M. Duckett
Partner

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

EXECUTIVE SUMMARY

We conducted a performance audit of Equal Employment Opportunity Commission's (EEOC) Personnel Security Program for calendar year 2013. Our audit was performed in accordance with generally accepted Government Auditing Standards. Accordingly, our audit included examining, on a test basis, evidence about EEOC's compliance with Title 5 of the Code of Federal Regulations (CFR) Part 731 and 32 CFR Part 2001 and performing such other procedures as we considered necessary.

Overall the objective of this audit was to ensure that EEOC has implemented a Personnel Security Program that adheres to policies and procedures as described by the Office of Personnel Management (OPM) and the Code of Federal Regulations as well as to determine whether EEOC's personnel security program was effective and efficient.

Although EEOC has designed an overall compliant personnel security program, we identified areas in which improvements are needed in the implementation of the program in order to achieve optimum effectiveness and efficiency.

- Classified Information Management,
- Suitibility Determinations, and
- Physical Security and Credentialing

Without such improvements, EEOC runs the risk of insufficient oversight, inadequate practices, and unauthorized disclosure of classified information. Also, not implementing these improvements to the personnel security program may result in individuals holding positions for which they are not suitable or fit, and limiting EEOC's ability to protect national security, privacy-related information, and national interest. The conditions noted were caused by a lack of EEOC policies and procedures for classified information and ineffective implementation of established requirements.

Our seventeen recommendations call for management to develop or update policies and procedures, to implement those policies and procedures, to adhere to the requirements already in place, to address staffing concerns within the Office of the Chief Human Capital Officer (OCHCO), and to complete risk designations, reinvestigations, and OPM reporting in accordance with the requirements.

BACKGROUND

The U.S. 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), national origin, age (40 or older), disability or genetic information. It is also illegal to discriminate against a person because the person complained about discrimination, filed a charge of discrimination, or participated in an employment discrimination investigation or lawsuit. The EEOC carries out its mission through its headquarters office in Washington, D.C. and through 53 field offices serving every part of the nation.

The Personnel Security Program is managed by the EEOC's, Office of Chief Human Capital Officer (OCHCO). The EEOC conducts personnel security investigations to determine if applicants, interns/volunteers, contractors, and employees meet the suitability requirements for employment. The scope of a personnel security investigation varies depending on the duties and access requirements for the position. The authority to conduct personnel security investigations is derived from Executive Order 10450, Security Requirements for Government Employment, and Title 5, Code of Federal Regulations (CFR), parts 731 and 736.

Per EEOC order 530.010, EEOC must "ensure that personnel security investigations are conducted in accordance with 5 CFR 736. Suitability determinations shall be made for employment in covered positions in accordance with 5 CFR 731. Fitness determinations shall be made for employment in the excepted service in accordance with 5 CFR 302.203. Fitness determinations shall be made for contract employees in accordance with the Office of Personnel Management's (OPM) Supplemental Credentialing Standards." Agency personnel shall be credentialed in accordance with Federal Information Processing Standards (FIPS) 201 (as amended), Office of Management and Budget (OMB) Memo 05-24, USAccess policy, and the OPM Final Credentialing Standards Memorandum (as amended). The EEOC maintains and safeguards personnel security investigations and materials related to adjudications in strict confidence. Access is granted only to authorized individuals, and handled in accordance with the Privacy Act of 1974, 29 CFR 1611.15, and EEOC Order 531.001.

EEOC established a project team and implemented the agency's HSPD-12 policy. The Office of Information Technology (OIT), the Office of Chief Financial Officer (OCFO), and Office of the Chief Human Capital Officer (OCHCO) jointly sponsored the implementation. OCHCO has lead responsibility for background investigations, adjudication, and PIV card issuance/maintenance. OCFO has lead responsibility for implementing use of the PIV credentials for facility access. However, the field offices have been delegated the implementation of credentialing for facility access. OIT has lead responsibility for implementing use of the PIV credentials for logical access to EEOC information technology networks.

EEOC background investigations are conducted by OPM, Federal Investigative Services (FIS). The extent of the background investigation is determined by the type of information individuals will have access to. EEOC uses OPM-FIS background investigations as the basis for its suitability determinations for employment in covered positions. All positions subject to investigation under this part must also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive, when appropriate. This designation is complementary to the risk designation, and may have an effect on the position's investigative requirement. Procedures for determining investigative requirements for all positions based upon risk and sensitivity are published in OPM issuances, as described in 5 CFR 731.102(c).

In the EEOC Personnel Security and Suitability Handbook, EEOC has designated most positions as Non-sensitive for national security purposes, which indicates that classified information is not generated, handled or stored by EEOC positions. However, some EEOC employees are required to handle classified information related to EEO complaints filed against intelligence agencies. Some of this classified information is stored at EEOC headquarter and field office locations. Currently, there is no classified information policy nor is classified information being managed by a singular office. Instead, EEOC's classified information is managed by the individuals and offices handling the information such as the Office of Federal Operations (OFO), the Office of Field Programs (OFP), and Washington Field Office (WFO).

RESULTS OF AUDIT

Although EEOC has designed an overall compliant Personnel Security Program, we identified the following areas in which improvements are needed in the implementation of the program in order to achieve optimum effectiveness and efficiency:

- Classified Information Management,
- Suitibility Determinations, and
- Physical Security and Credentialing

Without such improvements, EEOC runs the risk of insufficient oversight, inadequate practices, and unauthorized disclosure of classified information. Also, not implementing these improvements to the personnel security program may result in individuals holding positions for which they are not suitable or fit, and limiting EEOC's ability to protect national security, privacy-related information, and national interest.

Classified Information Management

Currently, EEOC does not have formal, documented policies and procedures to address the safeguarding, transfer, storage, or disposal of classified information. Also, a training policy for classified information has not been established. Classified information is managed by the individual offices and field offices based on verbal guidance from the originating federal agencies. The individuals working on the classified information generally work directly with the intelligence agency and receive feedback and instruction on how to handle the classified cases. Therefore, EEOC cannot provide assurance to the proper oversight, consistent training and safeguarding of classified information.

OCHCO has been delegated the responsibility of background investigations and adjudications. Clearances for the employees who handle classified information are initiated by the intelligence agency that works directly with the EEOC employee or his/her supervisor to obtain the information necessary for the clearance process. The employee information is submitted to the intelligence agency that conducts the investigation and renders an adjudication decision. However, the current process for initiating, granting and monitoring security clearances, need-to-know and security clearance access levels to classified information are not within OCHCO or any other singular office within EEOC HQ. As a result, OCHCO is not aware of the sensitivity of the information to be accessed, the clearances obtained, or the clearance level required to handle the classified information.

Approximately 18 EEOC employees, primarily in OFO, OFP, and WFO, currently have access to classified information as a result of EEO complaints filed against intelligence agencies. The classified information is stored either as hard copy or on thumb drives provided by the originating intelligence agency. Each employee and/or their office is responsible for the safeguarding and proper handling of the classified information. EEOC Staff interviewed reported that procedures for safeguarding classified information are communicated verbally to them by the intelligence agency or by their agency point of contact within EEOC. Guidance is also provided to cleared EEOC employees at meetings with the originating agency. None of the EEOC staff interviewed reported a formal EEOC-provided or mandated training for individuals who require access to classified information. OFO stated that they are planning to develop a policy and procedure document to cover the handling of classified information within their office. The development of this document is still in its early stages and the completion date is not yet known.

OIT requires all employees to complete a security awareness training each year. This EEOC-developed training does not cover handling, use, or transfer of classified information. OIT stated that they did not include classified information in the security awareness training due to the small number of employees who handle classified information. There is no EEOC requirement that individuals who handle classified information receive additional training in this area.

According to the staff interviewed, the classified information is stored in GSA Security Containers at EEOC Headquarters and at WFO. We were told that at least one field office stored classified information at their location, however the exact number of field offices with classified information was not provided to us prior to the end of fieldwork.

Executive Order 13526, Classified National Security Information, section 5.4 requires agencies that handle classified information to designate a senior agency official to direct and administer the program. This official is responsible for establishing and maintaining security education and training programs, establishing and maintaining a self-inspection program, establishing procedures to prevent unnecessary access to classified information, and accounting for the costs associated with implementing this program and reporting them to the Director of the Information Security Oversight Office.

EEOC designated all personnel positions as "Non-sensitive" for national security purposes which would indicate that the information handled by those individuals would not be of a classified nature. Also OCHCO was unaware until recently of higher level security clearances held by several employees as a result of the classified information. EEOC relies on the guidance provided to the user by the originating agency in lieu of developing its own procedures.

Consequently, EEOC did not develop classified information policies and procedures and each office manages its classified information without the benefit of oversight or guidance from the required designated senior agency official in accordance with Executive Order 13526 and 32 CFR Parts 2001 & 2003. Although several office directors and users of classified information have stated that they believe instituting a cohesive, agency-wide classified information management policy would be beneficial, no specific office has taken responsibility for developing one. Without a personnel security policy that includes classified information management, the EEOC runs the risk of insufficient oversight, inadequate practices, and unauthorized disclosure of classified information.

Recommendation:

We recommend that EEOC Senior Management direct the Office of the Chief Human Capital Officer and the Office of the Chief Financial Officer work together to:

1. Identify all HQs and Field Offices where classified national security information is safeguarded, handled, processed, reproduced, transmitted, transported, or destroyed.

2. Identify all EEOC employees with:

    a. current or prior access to classified national security information;

b. a current adjudicated security clearance and the sponsoring agency, if applicable; and
c. special access or interim clearance and the sponsoring agency, if applicable.

3. Develop and implement policies and procedures to address the safeguarding, transfer, storage, or disposal of classified information. The policy should include the requirements for Memorandums of Understanding between agencies.

4. Designate a senior agency official to direct and administer the program in accordance with Executive Order 13526 and 32 CFR Parts 2001 & 2003. This senior agency official/office must be provided the resources and authority to achieve compliance with the requirements associated with Classified National Security Information program.

5. Implement a formalized training program for individuals who use classified information as a part of their duties. If an external agency is to assume the responsibility of training these individuals, this agreement should be documented in an MOU.

6. Perform and document an assessment/evaluation of current classified information practices and safeguarding at headquarters and field offices to determine any non-compliances. Immediate corrective action should be taken to address any non-compliances noted.

7. Incorporate a review of controls over classified information in EEOC's annual Federal Managers Financial Integrity Act (FMFIA) process.

Management Response:

OCHCO Response: The EEOC suitability program is design to adhere to applicable regulations, executive orders, and statues regarding suitability and fitness determinations; each covered position is designated non-sensitive. Currently, there are no covered positions that fall under Executive Order 12968 (National Security positions) eligibility for access to classified information.

OFP Response: Currently only eight administrative judges (AJ) have clearances or authorization issued from intelligence agencies (IA). A survey of those individuals reveals that they rarely have access to classified information. In addition, classified documentation is ordinarily redacted or is reviewed at FBI offices. AJs follow the procedures established by the IA.

OFO Response: Each office that has some involvement with classified information is managed by a senior official.

OCFO Response: Overall, OCFO agreed with the finding. At this present time, the sponsoring intelligence agencies and EEOC do not have an MOU/MOA established to address the required continual monitoring, evaluation or reporting of an EEOC employees continued eligibility, or need-to-know of classified information. This is why it is important that the agency in custody of the classified information and handling the classified information manage its own employee's personnel security clearance process and adjudication, need-to-know and access in cooperation with the intelligence community agencies EEOC is serving.

OCFO also stated that their office has never received a thumb drive containing classified information. When thumb drives are used, they are only used to transmit draft decisions to the IA reviewing official. However, the possibility of classified information on unclassified computers is present.

See management's response in its entirety in **Appendix C**.

Auditor Analysis:

The lack of a unified response speaks to a decentralized process without a designated senior agency official responsible for the classified information and handling. The number of employees with access to classified information was obtained from EEOC's *PPD-19 Supplemental Response*, dated September 11, 2013. This number includes employees in OFO, OFP, and WFO. Also, the procedures for reviewing classified information differ between intelligence agencies. No consensus was reached about this issue and no responses were made to the corrective actions. Therefore, the recommendations remain open until management decision is reached with the EEOC OIG.

Suitability Determinations

We noted several instances where EEOC did not comply with federal requirements or its own policies and procedures pertaining to suitability determinations. These instances include:

- Risk Designations
- Reinvestigations
- Federal Personnel Payroll System
- Certificates of Investigation
- Reporting Adjudication Decisions to OPM

As a result, EEOC cannot provide assurance that there are no individuals holding positions for which they are not suited, thereby limiting EEOC's ability to protect national security, privacy-related information, and national interest.

Risk Designations

The EEOC has not conducted risk designations for all public trust position descriptions as required by OPM, federal regulations, and EEOC policy. Currently only six of an estimated 200 covered positions have received a risk designation. Risk designations have been required by 5 CFR 731.106(a) since 2008. The EEOC began performing risk designations in 2011, however the designations have only been performed for six employees.

Title 5, CFR Section 731.106 and EEOC Order 530.010 both require EEOC to designate every covered position within the agency at a high, moderate, or low risk as determined by the position's potential for adverse impact to the efficiency or integrity of the service. In addition, all positions subject to investigation must also receive a sensitivity designation of special-sensitive, critical-sensitive, or noncritical sensitive, when appropriate.

OCHCO personnel stated that due to low staffing levels they decided to complete risk designations for new hires only. Also, OCHCO has decided to wait until OPM and the Office of the Director of National Intelligence (ODNI) promulgate new joint regulations on sensitive positions and update or replace the Automated Position Designation Tool before they perform any additional risk designations.

Without a corresponding risk designation for all covered positions, EEOC is at risk of maintaining the wrong level of investigation for covered positions. This could result in individuals holding positions for which they are not suitable, limiting EEOC's ability to protect national security, privacy-related information, and national interest.

Reinvestigations

EEOC does not consistently conduct reinvestigations for employees in public trust positions as required by federal regulation and EEOC policy. According to EEOC Order 530.010 and 5 CFR 731.106, EEOC must ensure reinvestigations are conducted for persons occupying public trust positions at least once every five years. Of the 25 employees selected for testing who should have had at least one reinvestigation, 11 had not had a reinvestigation completed in the last 5 years. The amount of time between investigations for these employees ranged from 6 to 28 years, with an average of 9 years. Additionally, EEOC could not locate the reinvestigation records of three of the 25 employees selected, so we were unable to determine whether they received a reinvestigation or not.

Although EEOC has a written policy requiring reinvestigations, the OCHCO has elected not to implement reinvestigation procedures because OPM has not issued implementation guidance to federal agencies regarding public trust reinvestigations.

Without conducting periodic reinvestigations for current public trust positions once every 5 years, the EEOC could potentially have unsuitable personnel conducting EEOC activities.

Federal Personnel/Payroll System (FPPS)

The EEOC has not completely entered employee investigation data, such as dates and type of adjudication completed, into FPPS although it is required by EEOC's Personnel Security Program Order, Chapter 1. OCHCO is charged with the responsibility of maintaining the completeness of FPPS for all EEOC Federal employees. Out of 21 EEOC employees selected for testing, eleven employee FPPS files had not been updated to show the type of investigation, and date of adjudication.

We also noted that the EEOC policy related to FPPS does not, but should, include a timeline for updating FPPS with the appropriate information, for example within 30 days after the adjudication date.

OCHCO has not implemented proper procedures to ensure that FPPS is updated with the results of adjudication in a timely manner. By not updating the FPPS to include investigation information, the EEOC is limiting its ability to track and maintain the necessary data related to suitability determinations.

Certificates of Investigation

The EEOC did not maintain a Certificate of Investigation (COI) within each current employee's electronic Official Personnel Folder (eOPF), as required by OPM and EEOC Order 530.010, Chapter 5 and The *Office of Personnel Management (OPM) Operating Manual: The Guide to Record Keeping, Section 3-E*. Although internal tracking documents showed that an investigation was performed, we were not provided a COI for 16 of the 50 employees selected for testing. The OCHCO is responsible for maintaining EEOC employee's eOPF and receiving and signing the COI.

OCHCO stated that it is experiencing a staffing shortage that is affecting the maintenance of eOPF records. Therefore, EEOC employees' eOPF files do not include the necessary information to document that an appropriate background investigation was performed. This could impact an employee's clearance documentation when transferring to another agency. Also, without this information, EEOC may not be able to validate whether the appropriate type of investigation was obtained.

Reporting Adjudication Decisions to OPM

EEOC did not provide evidence that they reported adjudication decisions to OPM as required by the 5 CFR 731.206 and EEOC Order 530.010, Chapter 5. We selected 25 employees for testing

and requested evidence showing that EEOC reported the employees' adjudication decisions to OPM as required. We were not provided evidence of reporting for any of these employees prior to the end of fieldwork.

Without proper mechanisms to access information in a timely manner, EEOC is not able to demonstrate compliance with federal reporting requirements.

EEOC has designed the proper system to meet the federal personnel security program requirements. However, EEOC has not effectively and consistently implemented the policies and procedures as outlined. As a result, EEOC is not able to demonstrate compliance or provide assurance that there are no individuals holding positions for which they are not suited, thereby limiting EEOC's ability to protect national security, privacy-related information, and national interest.

Recommendations:

We recommend that the Office of the Chief Human Capital Officer:

8. Complete risk designations for the remaining estimated 194 EEOC covered positions.

9. Complete and begin any outstanding reinvestigations as required by the CFR.

10. Adhere to EEOC policy and federal requirements pertaining to reinvestigations. EEOC should follow their internal policy until further guidance is provided by OPM.

11. Update the policy for the Federal Personnel Payroll System with a timeline and implement the revised standard.

12. Review all employee eOPFs to ensure proper inclusion of the employee's COI and in instances where the documentation is missing, insert the COI.

13. Report any outstanding EEOC adjudication decisions to the Office of Personnel Management and going forward adhere to the 90 day timeline.

14. Develop and implement a procedure to maintain relevant evidence documenting that the EEOC has informed OPM of the adjudication decisions it has made.

15. Explore and document the decision on using alternative staffing options, such as contract employees, part time employees, or obtaining an employee on detail in order to become current on risk designations, reinvestigations, FPPS, COIs, and adjudication reporting.

Management Response:

OCHCO Response: OCHCO management concurred with all findings and recommendations noted in this section. EEOC has employed a Personnel Security Specialist and Personnel Security Assistant to assist with these efforts. Corrective actions have begun on the recommendations and will be completed by the second quarter of FY 2015 except EEOC has decided to delay reinvestigations until such time as OPM issues guidance.

See management's response in its entirety in **Appendix C**.

Auditor Analysis:

We believe that the above-mentioned actions, if properly implemented, will resolve the condition and address the recommendations.

Physical Security and Credentialing

EEOC's HSPD-12 implementation plan establishes the OCFO as having the lead responsibility for implementing use of the PIV credentials for facility access across the agency. EEOC's physical security program is managed by OCFO. We noted that EEOC's physical security process is highly decentralized. The field offices have a great amount of autonomy as it relates to implementing security measures at their locations and the agency physical security manager has limited authority related to the security measures at field office locations.

EEOC has a headquarters and 53 field offices located throughout the United States. Each field office or district office establishes and manages its own physical security and credentialing process. There is currently insufficient coordination and review by headquarters to ensure compliance with EEOC physical security and credentialing requirements. As a result, EEOC is increasing the risk that a security breach could occur that would affect the safety of employees or the information they handle.

We asked field office staff about the physical security measures at their respective locations and compared these measures to the physical security standards issued by the Interagency Security Committee (ISC) in their *Physical Security Criteria for Federal Facilities.* These standards, issued in 2010, set forth a baseline set of physical security measures to be applied to all Federal facilities based on their designated Facility Security Level (FSL). For multi-tenant buildings under GSA control, a representative from each tenant participates in the buildings' Facility Security Committee. The Facility Security Committee determines which building security measures to implement by a vote of the members. If the committee decides not to implement specific physical security measures, it is required to document its acceptance of the associated risk.

Security requirements for each location vary based on each office's FSL as described in the Interagency Security Committee's *Facilities Security Criteria*. We performed inquiries of nine field offices with various FSLs to determine whether the security measures in place at their location were in line with the security requirements of their FSL. We noted that four of the nine field offices did not fully comply with the security requirements for their FSL.

There is currently no review being performed by the physical security manager to ensure field office security measures and credentialing are in compliance with federal regulations.

Facilities Security Criteria for Federal Facilities, An Interagency Security Committee Standard sets forth certain *Facility Entrance Security Criteria* that Federal agencies must follow, specifically as it relates to badge identification, employee and visitor access control, and occupant and visitor screening based on their FSL. In all cases, the project documentation must clearly reflect the reason why the necessary protection cannot be achieved. It is extremely important that the rationale for accepting risk be well-documented, including alternative strategies that are considered or implemented, and opportunities in the future to implement necessary protection.

EEOC has not established an effective centralized method for ensuring field office compliance with physical security and credentialing regulations. Due to its relatively small size and diversity of locations, physical security is managed at the field-office level and there is little to no coordination or consultation with security staff at EEOC headquarters regarding physical security and credentialing. In addition, EEOC does not perform regular reviews of the security measures in place at field office locations to ensure they are appropriate for each field office's FSL. Field offices are required to submit an annual security self-assessment checklist, however this checklist does not include aspects such as building access, badging, visitor access, and visitor and employee screening.

The lack of cohesive physical security, credentialing, and tools for consistent application has resulted in inconsistent physical security practices across EEOC's field office locations. Oversight provided by OCFO is not robust enough to properly mitigate the risk associated with such a decentralized structure. Without proper oversight by the Physical Security Manager to ensure field office compliance with security directives, EEOC is increasing the risk that a security breach could occur that would affect the safety of employees or the information they handle.

Recommendation:

We recommend that the Office of the Chief Financial Officer:

16. Update and implement comprehensive policies and procedures for physical security. These policies and procedures should include but not be limited to:

a. Providing training for the FSC member or designee at each field office location at least annually;
b. Developing and implementing a field office onsite security assessment program, that includes performing assessments and/or spot checks of field office security measures by the OCFO on a rotational basis as it relates to Interagency Security Committee requirements; and
c. Assisting and ensuring field offices correct noted security weaknesses or document acceptance of risk where EEOC has determined corrective action will not be taken.

17. Revise the field office self-assessment checklist to include facility security and credentialing information.

18. Immediately correct any known weaknesses. If EEOC determines not to correct a noted weakness, EEOC should document this analysis and their acceptance of the associated risk.

19. Increase coordination between OCFO and OFP to improve field office security posture, awareness and training to ensure compliance with applicable EEOC orders and guides; *Facility Security Committees*, An ISC Standard, dated January 1, 2012, 2nd edition; and other applicable Interagency Security Committee Standards. .

Management Response:

OCFO Response: OCFO concurred with the intent of the recommendations with a few minor clarifications. OCFO management stated that EEOC can only impose EEOC specific requirements on EEOC controlled space. It is the Facility Security Committee's responsibility to ensure that security procedures and countermeasures at each facility/building are administered properly, to include entry access control. Corrective actions will be implemented in FY 2015.

See management's response in its entirety in **Appendix C**.

Auditor Analysis:

We believe that the above-mentioned actions, if properly implemented, will resolve the condition and most recommendations. However, the OCFO response did not address recommendations 16c or 18. They will remain open until addressed with the OIG.

Appendix A: Glossary of Acronyms

CFR	Code of Federal Regulations
COI	Certificate of Investigations
COO	Chief Operating Officer
DHS	Department of Homeland Security
EEOC	U.S. Equal Employment Opportunity Commission
eOPF	Electronic Official Personnel Folder
FIPS	Federal Information Processing Standards
FIS	Federal Investigative Services
FOUO	For Official Use Only
FSL	Facility Security Level
FPPS	Federal Personnel/Payroll System
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
ISC	Interagency Security Committee
IT	Information Technology
OCFO	Office of the Chief Financial Officer
OCHCO	Office of the Chief Human Capital Officer (formerly OHR)
ODNI	Office of the Director of National Intelligence
OFO	Office of Federal Operations
OFP	Office of Field Programs
OHR	Office of Human Resources (now OCHCO)
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIV	Personal Identity Verification
WFO	Washington Field Office

Appendix B: Objectives, Scope, and Methodology

OBJECTIVES

The overall objective of our audit was to determine whether EEOC has implemented a personnel security program that adheres to policies and procedures as described by the Office of Personnel Management and the Code of Federal Regulations.

More specifically, the objectives of our audit were as follows:

1. To ensure that the EEOC Personnel Security Program Handbook provides guidance on the procedures, rules, roles, and responsibilities involved in the personnel security investigation process.
2. To ensure as stipulated by 5 CFR 736.201, that personnel security investigations are initiated within 14 days of placement in the position.
3. To ensure that EEOC, as stipulated by 5 CFR 731.106, conducts reinvestigations and a determination regarding continued employment of persons occupying public trust positions at least once every 5 years.
4. To ensure that EEOC reports to OPM the level or nature, result, and completion date of each background investigation or reinvestigation, each agency decision based on such investigation or reinvestigation, and any personnel action taken based on such investigation or reinvestigation, as required in OPM issuances.
5. To ensure that a copy of the Certificate of Investigation shall be placed in the employee's electronic Official Personnel Folder (eOPF).
6. To ensure that the type of investigation and the date of adjudication are reported in the Federal Personnel/Payroll System (FPPS)
7. To ensure that EEOC has implemented a process of risk designation.
8. To ensure that EEOC has implemented the appropriate procedures associated with risk level changes.
9. To review whether EEOC has classified information.
10. To ensure that, when applicable, EEOC has implemented the appropriate policies and procedures, as prescribed by federal statute, associated with individuals who may have access to classified information that is maintained and used on the behalf of another agency.
11. To assess the effectiveness and efficiency of EEOC's personnel security program and to identify best practices and provide areas for improvement.

SCOPE AND METHODOLOGY

The scope of our audit included all federal established guidance and best practices associated with the implementation of an effective and efficient Personnel Security Program. Our audit focused on the appropriateness and effectiveness of EEOC's Personnel Security Program during calendar year 2013.

We used a four-phased approach: planning, internal control assessment, testing, and reporting. We used IDEA sampling software to make our sample selections and perform testing when reasonable. We reviewed key applicable laws and regulations. We interviewed EEOC staff to document the processes and procedures and tested those processes and procedures to ensure they were operating effectively. We researched and identified best practices and identified areas for improvement.

We noted exceptions and wrote findings in those instances where violations occurred and were not corrected, where internal control weaknesses existed, and where processes were determined not to be effective and efficient. We stated the conditions, causes and effects of our findings, as well as the criteria upon which the findings were based, and recommendations for correcting the issues.

Appendix C: Management Response

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

Office of the Chair

August 18, 2014

MEMORANDUM

TO: Milton A. Mayo Jr.
Inspector General

FROM: Claudia A. Withers
Chief Operating Officer

SUBJECT: EEOC Response to OIG Draft Report 2013-08-PSA—Performance Audit of the Agency's Personnel Security Program

Thank you for the opportunity to provide comments to the above captioned report and for providing an extension to August 15th to enable coordination of the response. Attached are comments and responses to the report for your review and consideration. Due to the comprehensiveness of the report, we have decided to provide the comments of each affected office in total rather than combining them into one narrative. Please do not hesitate to contact me if you have any further questions.

From the Office of the Chief Human Capital Officer:

Report – Performance Audit of the Agency's Personnel Security Program (OIG Report Number 2013-08-PSA) conducted by the EEOC IG.
Response: The EEOC suitability program is design to adhere to applicable regulations, executive orders, and statues regarding suitability and fitness determinations; each covered position is designated non-sensitive. Currently, there are no covered positions that fall under Executive Order 12968 (National Security positions) eligibility for access to classified information.

Recommendations to the Office of the Chief Human Capital Officer from the EEOC IG:
Action: Complete risk designations for the remaining estimated 194 EEOC covered positions (IG):
Response: Designations for 85% of our positions have been completed. To meet the requirement with ensuring that every position within the EEOC is designated at a high, moderate, and low risk level as determine by the position's potential impact that could adversely impinge on the efficiency and integrity of the EEOC; we plan to have this completed by the end of the second quarter of FY 2015.

Action: Complete and begin any outstanding reinvestigations as required by the CFR (IG):

131 M Street, N. E., Suite 6NW08F Phone (202) 663-4001 TTY (202) 663-4141 FAX (202) 663-4110 JACQUELINE.BERRIEN@EEOC.GOV

Response: Currently, OPM-Federal Investigative Service (FIS) is advising agencies that it is acceptable to delay implementing public trust reinvestigations; OPM-Federal Investigative Service (FIS) is not assessing agencies implementation of the Executive Order and regulations pertaining to the reinvestigation requirements for positions of public trust, but are planning to issue implementing guidance once the proposed 5 CFR Part 1400 regulation (which includes reinvestigation requirements for sensitive positions) is finalize.

In accordance with the memorandum issued by OPM-FIS dated April 30, 2014, OPM is implementing a phased deployment of tiered investigations; required to achieve full operating capability (FOC) by the end of fiscal year 2017. A Federal Investigative Standards (FIS) Working Group is currently revising the investigative standards to align national security and suitability investigations to the extent possible in accordance with E.O. 13467 "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information."

It is the intent of OPM-FIS to direct phase deployment of a tiered background investigation process which builds upon background investigations conducted at lower tiers in an integrated and collaborative manner across all federal agencies. The increased alignment will enhance consistency and efficiency, making government investigations more timely and cost-effective and improving reciprocity.
Early initial operating capability (IOC) for federal agencies to implement the tiered background investigation process is as follows:

> IOC for Tiers 1 and 2 (Low Risk and Moderate Risk) is October 2014.
> IOC for Tier 3 (Non-Critical Sensitive, L, Confidential, and Secret) is October 2015.
> IOC for Tiers 4 and 5 (High Risk-Public Trust and Top Secret / Special Secret) is October 2016.

The goal is all tiers will reach FOC by the end of the fiscal year 2017. Therefore, we have been advised that implementing the reinvestigation requirements prior to the issuance of further guidance from OPM-FIS is **not discouraged or encouraged**.
Because, the position designations play a vital role in the process and based on the fiscal impact this could have on our budget, we have decided to await final regulations in this area.

Action: Adhere to EEOC policy and federal requirements pertaining to reinvestigations. EEOC should follow their internal policy until further guidance is provided by OPM (IG):
Response: Our internal policy only speaks to the fact that we are required to conduct reinvestigations; however, we notified employees as required about this new procedure and informed them that we are waiting further instruction in a memorandum dated October 31, 2013. The language is as quoted "Please note that while the public trust reinvestigation requirement *§731,106(d) has been in effect since November 2011, OPM has yet to issue implementation guidance to federal agencies in regards to public trust reinvestigations. As such, OCHCO is not conducting these reinvestigations until such time as OPM issues their implementation guidance to federal agencies. Currently, OPM does not have a timeline for issuing their implementation guidance."*

Action: Update the policy for the Federal Personnel Payroll System with a timeline and implement the revised standard (IG):
Response: This is considered a procedure; therefore, we will develop Standard Operating Procedures to ensure that we document the procedures for annotating required documents. We will have this completed by the end of the first quarter of FY 2015.

Action: Review all employee eOPFs to ensure proper inclusion of the employee's COI and in instances where the documentation is missing insert the CO (IG):
Response: We will review personnel security files for Certificates Of Investigation (COI). If the COI is missing, we will verify e-OPF for the COI or verify the completion and adjudication of the background investigation utilizing the Clearance Verification System (CVS). CVS produces an automated version of the COI that is maintained with OPM-FISD. Therefore, we will download and print the findings and scan it into the employees' e-OPF.
We will also utilize the EEOC Employee Alpha Listing or some form of personnel roster/data to ensure the accuracy of the required information. We propose to have this completed by the end of second quarter of FY 2015.

Action: Report any outstanding EEOC adjudication decisions to the Office of Personnel Management and going forward adhere to the 90 day timeline (IG):
Response: This is currently being addressed with the new-hire, Personnel Security Specialist; going forward we plan to adhere to the OPM requirement of the 90 day timeline. It is reflected in our 2013 assessment conducted by OPM (attached) which shows much improvement over this process since the report in 2010.

Action: Develop and implement a procedure to maintain relevant evidence documenting that the EEOC has informed OPM of the adjudication decisions it has made (IG):
Response: This will also be included in the Standard Operating Procedures we will develop. Given that we have CVS access, we are able to inform OPM of our adjudication decisions electronically. In those cases that we must do it manually, we will continue to use the INV FORM 79A.
In addition, we will continue to maintain a personnel security file for employees, contractors, and affiliates that have a completed background investigation which will consist of:

Cover sheet (snap shot of background investigation information)
COI or the automated version (with background information provided by OPM-FIS)
Resume
OF306
Signature pages (from the e-QIP background investigation application)

Action: Explore and document the decision on using alternative staffing options, such as contract employees, part time employees, or obtaining an employee on detail in order to become current risk designations, reinvestigations, FPPS, COIs, and adjudication reporting (IG):
Response: We will explore these possibilities as needed now that we have employed a Personnel Security Specialist and Personnel Security Assistant. Final decision will be made at the completion of our action plan.

From the Office of Field Programs:

Under the heading Classified Information Management, the report raises concerns that EEOC does not have "formal, documented policies and procedures to address the safeguarding, transfer, storage or disposal of classified information." The report indicates that EEOC has approximately 18 employees who "currently have access to classified information as a result of EEO complaints filed against intelligence agencies."

Our records show that there are a total of 8 Administrative Judges (AJs) who have security clearances or some form of authorization issued by one or more of the intelligence agencies, most by the FBI. A survey of those individuals reveals that they rarely have access to classified information. Most indicated that over the course of the last three years they have not had a case in which the agency indicated that the file contained classified information as contemplated by Executive Order 13526 (i.e., national security information). In those rare instances where an AJ has handled a complaint in which the respondent agency indicated that the eeo investigative file or other documents relevant to the case contained classified or sensitive information, the documents were redacted before being provided to the AJ. In a few instances, the AJ viewed the documents onsite at the respondent agency.

With respect to the handling of the investigative file from intelligence agencies, the AJs follow the procedures established by the agency submitting the eeo investigative file. This includes such things as the AJ being the only person who can access the file, requiring that decisions by the AJ be reviewed by the agency before being issued to the complainant to ensure that no "classified information" is included in the decision and using aliases for certain individuals identified in the investigative record. In the WFO and the SFDO all such documents are maintained in a safe with only those AJs with security clearances, or otherwise authorized by the respondent agency, having access.
It is important to note that the intelligence agency, not the EEOC, conducts the necessary background checks, issues the security clearance and provides the necessary training. Additionally, the respondent agency controls the manner of access to the documents as well as the level of access.

From the Office of Federal Operations:

Page 3 of the draft states that "In the EEOC Personnel Security and Suitability Handbook, EEOC has designated all positions as Non-sensitive for national security purposes…" This statement is repeated on page 5 of the draft. However, in looking at the Handbook that I found on InSite, on page 3, it states "The majority of EEOC positions are non-sensitive…." I could not locate a statement that indicates all positions have been designated as Non-sensitive.

Later, that paragraph states that "…some EEOC employees are required to handle classified information related to EEO complaints filed against intelligence agencies." In OFO, the staff handles appeals in which classified information has been redacted; classified information is not handled.

Also, in that same paragraph on page 3 of the draft, there are errors in identifying the Office of Federal Operations and the Office of Field Programs.

On page 5, the 4th paragraph reads: "Consequently, EEOC did not develop classified information policies and procedures and each office manages its classified information without benefit of oversight or guidance from senior EEOC officials." This is incorrect in that each office that has some involvement with classified information is managed by a senior official. The statement incorrectly implies that there are no controls over the process.

From the Office of the Chief Financial Officer:

The Office of the Chief Financial Officer (OCFO) fully understands that the protection of Classified National Security Information is critical to our Nation's security and national interests. Executive Order 13526, *Classified National Security Information* (December 29, 2009), the Code of Federal Regulation (CFR) 32 CFR Parts 2001 and 2003, *Information Security Oversight Office: Classified National Security Information; Final Rule* (June 28, 2010) and multiple Intelligence Community Directives (ICDs) from the Office of the Director of National Intelligence specifically state requirements for the storage, access, handling, processing, marking, transporting and destruction of Classified National Security Information, to include required training, reporting, documents and program management.

The OCFO, Central Services Division (CSD), supports the mission of the Equal Employment Opportunity Commission (EEOC) with a Supervisory Security Specialist and two Security Specialists. At this present time the OCFO/CSD oversee the functions of life safety, physical security, emergency preparedness and continuity of operations for Headquarters (HQ) and all Field Offices, in cooperation with the Office of Field Programs. The OCFO/CSD does not have oversight of the Classified National Security Information program.

Following are OCFO's comments and recommendations on the Draft Report-Performance Audit of the Agency's Personnel Security Program (OIG Report Number 2013-08-PSA).

Page/Paragraph	Comments and Recommendations
Page 4/Para 2	*"Clearances for the employees who handle classified information are initiated by the intelligence agency that works directly with the EEOC employee or his/her supervisor to obtain the information necessary for the clearance process. The employee information is submitted to the intelligence agency that conducts the investigation and renders an adjudication decision."* **Comment:** Actually, our employees accessing classified national security information fall into two categories: (1) those with fully adjudicated security clearances by the respective sponsoring Intelligence Agency (IA); and those with "special access" or what is commonly referred to as an Interim Clearance, granted by the respective Intelligence Agency, which is primarily the case with the Central Intelligence Agency (CIA) classified cases and

	respective attorneys and administrative judges. However, these "special access" or interim clearances do not include a full review of security clearance eligibility requirements and adjudicative guidelines. In fact, some of these employees with "special access" or interim clearance have had that designation for 5 years or more; some employees granted full clearances or interim clearances no longer work at the agency and this was never reported to the sponsoring agency or that employee debriefed. **Recommendation: Replace with** "Security clearances and special access for the employees who handle classified information are initiated by the sponsoring Intelligence Agency that works directly with the EEOC employee or his/her supervisor to complete the necessary security clearance eligibility package. The employee information is submitted to the sponsoring Intelligence Agency that conducts the background investigation and renders an adjudicative decision and grants eligibility and access levels. ~~This entire process is void of any involvement by the OCHCO and up until recently, without the knowledge of the OCHCO."~~
Page 4/Para 2	*"However, the current process for increasing the clearance level needed to handle classified information does not include OCHCO."* **Comment:** At this present time, the sponsoring intelligence agencies and EEOC do not have an MOU/MOA established to address the required continual monitoring, evaluation or reporting of an EEOC employees continued eligibility, or need-to-know of classified information; especially when derogatory and/or disciplinary information or actions are self reported, discovered or reported and access to classified information should be removed, suspended or revoked. This is why it is important that the agency in custody of the classified information and handling the classified information manage its own employee's personnel security clearance process and adjudication, need-to-know and access in cooperation with the intelligence community agencies EEOC is serving. **Recommendation: Delete** "*…increasing the clearance level needed to handle classified information does not include OCHCO.*" **Replace with** "initiating, granting and monitoring security clearances, need-to-know and security clearance access levels to classified information are not within OCHCO or any other singular office within EEOC HQ."
Page 4/Para 3	*"The classified information is stored either as hard copy or on thumb drives provided by the originating intelligence agency."* **Comment:** A preliminary inquiry of the Classified National Security Information program was conducted by the Supervisory Security Specialist in August 2013 after it was learned that EEOC employee's were being sponsored and granted security clearances and that EEOC was in custody of

	Classified National Security Information. During that inquiry the only mention of the use of a thumb drive was by Todd Denicoff, attorney in the Office of Federal Operations (OFO), who worked with classified cases. Mr. Denicoff explained that when they write a draft decision on a classified case they sit down at their unclassified network workstation computer with the classified file and the redacted/unclassified file. They write their draft decision on the unclassified network workstation computer, using care to write/draft it as unclassified, paying close attention to the redacted/unclassified file. Mr. Denicoff stated that they use this process because often times the redacted/unclassified file is so "blacked-out" that they need the complete classified file to fully comprehend what has happened in the case to render a decision accurately. After the draft decision is completed it is either copied to a thumb drive, other removable media or printed, and then secured in the GSA-approved security container until it is delivered to the Intelligence Agency (IA) courier, usually these are CIA cases, and it is delivered to the IA reviewing official. Once it arrives at the respective IA it is given to a reviewing official that will closely read the draft decision to ensure that there is no classified information contained. Once approved by the IA reviewing official, then the EEOC can finalize or publish the decision. Therefore, there is the potential for classified information to be within the draft decision, which was created on an EEOC unclassified network workstation. This process described above involves a multitude of dangers, security violations and security infractions that are not addressed in this audit report. Finally, if an Intelligence Agency were to provide a thumb drive, or other removable media, with classified information on it…then the EEOC attorney would be accessing classified information on our unclassified network and EEOC would have a serious national security violation and classified spillage that must be reported to the Director of National Intelligence and Information Security Oversight Office immediately. The Supervisory Security Specialist spoke with Mr. Denicoff on July 24, 2014 about the thumb drive statement and Mr. Denicoff emphatically stated that to the best of his knowledge, his office has never received a thumb drive containing classified information from any Intelligence Agency. **Recommendation: Delete** the reference to a **thumb drive** being used to store classified information and being provided by the originating intelligence agency. **NOTE:** It is warranted to include a paragraph or comment about the process described above and the potential for classified information to be on the thumb drive containing the EEOC draft decision and that the draft decision is being written on the EEOC unclassified network and there is the potential for

	classified information to be in that draft decision.
Page 5/Para 4	*"Consequently, EEOC did not develop classified information policies and procedures and each office manages its classified information without the benefit of oversight or guidance from EEOC officials."* **Comment:** None **Recommendation: Delete** "EEOC officials" and **replace with** "the required designated senior agency official in accordance with Executive Order 13526 and 32 CFR Parts 2001 & 2003."
Page 5/ Recommendation	**CRITICAL** – there must be a recommendation that EEOC "designate a senior agency official to direct and administer the program" (i.e. Classified National Security Information) in accordance with Executive Order 13526, Sec. 5.4. **Comment:** It is critical that the audit report clearly state in the findings and/or recommendations that the EEOC must designate a HQ Office that will serve as the senior agency official to direct and administer the classified national security information program. Furthermore, this senior agency official/office must be provided the resources and authority to achieve compliance with the requirements associated with Classified National Security Information program.
Page 5/ Recommendation	*1. Identify all field offices that store or use classified information.* **Comment:** None **Recommendation: Delete** above recommendation language and **replace with:** 1. Identify all HQs and Field Offices where classified national security information is safeguarded, handled, processed, reproduced, transmitted, transported, or destroyed. 2. Identify all EEOC employees with (1) current or prior access to classified national security information; (2) a current adjudicated security clearance and the sponsoring agency, if applicable; and (3) special access or interim clearance and the sponsoring agency, if applicable. **NOTE:** Item #2 has implications for the OCHCO Personnel Security and Suitability Program functions and operations.
Page 10/ Physical Security	**Physical Security and Credentialing**

and Credentialing	**Comment:** It needs to be clearly defined in the introduction and scope on this topic that the auditors only looked at physical security as it related to credentialing (PIV cards or Agency photo ID) to entry access control and visitor access control to the facility/building and EEOC controlled space. Furthermore, the tenure of the draft report infers that EEOC has complete control over physical security at the field office locations, i.e. facilities/buildings…**and that is far from accurate**. EEOC has established policy and guidance in the EEOC Security Plan, Order 370.002 (currently under revision); Space Allocation Guidelines, and the Administrative Manual that addresses physical security measures, countermeasures and other standards. For example: Administrative Manual, Sec. 8.5, Identification and Access Control Card, addresses the proper procedures for wear, accountability and use of these cards for identification and entry access control, to include Federal Investigator Badges and Credentials. EEOC Security Plan, Order 370.002, addresses Physical Security in Appendix A, to include: Security Design Standards; Identification Badges; Security At Building Entrances; Duress Alarm Systems; Security Guard Services; Security Risk Assessments; and Security Planning. These topics also include collaboration with the General Services Administration (GSA), Federal Protective Services (FPS) and the Facility Security Committee (FSC, formerly known as the Building Security Committee) all of whom make recommendations and determinations about physical security and security countermeasures at federally-controlled buildings for multi-tenant occupants. The Space Allocation Guidelines goes into great deal addressing physical security measures in EEOC controlled space, to include: cipher locks, electric or electromagnetic locking devices, duress alarms, and entry access control of EEOC outer (public) and inner (staff) space. It is important to note that EEOC has addressed certain physical security measures and countermeasures, to include entry access control, but we can only impose EEOC specific requirements on EEOC controlled space. It is the Facility Security Committee's responsibility to ensure that security procedures and countermeasures at each facility/building are administered properly, to include entry access control. EEOC representation at each respective FSC is mandatory and addressed in a memorandum that was released on November 19, 2013 and FSC representatives are strongly encouraged to voice and vote on physical security measures and countermeasures that meet or enhance security of EEOC staff. Additionally, the FSC representative required training is being added to the EEOC Security

	Plan for implementation in FY 2015. **Recommendation:** The content of this report must clearly delineate the relationship between EEOC physical security requirements and the Facility Security Committee role, in partnership with Federal Protective Service for building/facility security, security countermeasures and entry access control.
Page 10/Para 1	*"We noted that EEOC's physical security process is highly decentralized."* **Comment:** This statement is not taking into account the role of the Facility Security Committee at each respective building/facility and designated Security Organization. **Recommendation: Delete** "process" and **add"**program requirements are limited to EEOC controlled space and the building/facility physical security program is significantly impacted by each field office locations Facility Security Committee voting decisions, where applicable, and technical advice/assistance provided by the designated Security Organization (i.e. Federal Protective Services) as explained in the *Facility Security Committees*, An ISC Standard, dated January 1, 2012, 2nd edition."
Page 11/ Recommendation	*"14. a. Providing required annual training for the security lead at each field office location;"* **Comment:** First, the only current security training requirement applicable to this topic is for FSC members and is found in the *Facility Security Committees*, An ISC Standard, dated January 1, 2012, 2nd edition, Sec. 4.6, Interagency Security Committee Training. There are four required training courses and it is not an annual requirement. **Recommendation: Delete** the term "annual" as it is not an annual requirement. FSC member training requirement was added to the EEOC Administrative Manual and the EEOC Security Plan, 370.002 (currently under revision) for implementation in FY 2015. Additionally, **delete** the term "security lead" and **replace with** "FSC member or designee. "
Page 11/ Recommendation	*"14. b. Performing annual assessments and/or spot checks of field office security measures by the OCFO on a rotational basis as it relates to Interagency Security Committee requirements; and"* **Comment:** Onsite annual security assessments of all field offices each year is not possible, fiscally or with regards to staffing. The OCFO has implemented onsite security assessments beginning August 2014 with a goal of four (4) field offices by the end of FY 2014. The current program goal is

	to achieve a minimum of five (5) onsite field office security assessments per fiscal year beginning in FY 2015. However, future budget constraints may require that we modify our plans. **Recommendation: Replace with** "Develop and implement a field office onsite security assessment program in coordination with the Office of Field Programs, to include announced and unannounced site visits, which will focus on increasing security posture and awareness at field office locations."
Page 11/ Recommendation	*"15. Revise the field office self-assessment checklist to include facility security and credentialing information."* **Comment:** The OCFO will continue the Annual Safety/Security Self Inspection program and will implement the recommendation of increasing more physical security and entry access control questions/assessments in the inspection criteria beginning FY 2015. Regarding relocations of EEOC space, we will continue to work with FPS and the prospective building's FSC to obtain the most current Facility Security Assessment (FSA) to ensure that physical security requirements meet the EEOC minimum standards. **Recommendation:** None
Page 12/ Recommendation	*"17. Increase the responsibility of the Physical Security Manager to improve the level of coordination and review of field office security measures to ensure compliance with EEOC physical security and credentialing requirements."* **Comment:** The Supervisory Security Specialist and Security Specialists already have all the necessary authority to meet the intent of this recommendation. **Recommendation: Delete this recommendation/finding. Replace with** "Increase coordination between OCFO and OFP to improve field office security posture, awareness and training to ensure compliance with applicable EEOC orders and guides; *Facility Security Committees*, An ISC Standard, dated January 1, 2012, 2nd edition; and other applicable Interagency Security Committee Standards.

cc: Nicholas Inzeo
Germaine Roseboro
Lisa Williams
Carlton Hadden
Kimberly Hancher