REPORT ON FISCAL YEAR 2008 INDEPENDENT AUDIT OF EEOC PRIVACY PROGRAM AUDIT REPORT NUMBER # 08-12-AEP

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

September 30, 2008

Ms. Aletha L. Brown
Inspector General
Equal Employment Opportunity Commission
1801 L Street, N.W.
Washington, D.C. 20507

SUBJECT:Subject: Report on Fiscal Year 2008 Independent Audit of the EEOC's Privacy Program; Report Number 08-12-AEP

Dear Ms. Brown:

In accordance with terms of the subject task order, Cotton & Company LLP conducted an audit of privacy and data protection policies and procedures used by the Equal Employment Opportunity Commission (EEOC). The audit included assessing compliance with applicable federal security and privacy laws and regulations, as well as a review of the EEOC's policies and procedures related to identifying and securing privacy-related data.

We interviewed key personnel involved in identifying and protecting personally identifiable information, and reviewed documentation supporting EEOC's efforts to comply with federal privacy and security laws and regulations. We identified specific control weaknesses and deficiencies, and developed recommendations designed to improve EEOC's compliance with federal privacy and security laws and regulations.

We conducted the audit in accordance with *Government Auditing Standards*. We were not engaged to and did not perform a financial statement audit, the purpose of which would be to express an opinion on specified elements, accounts, or items. This report is intended to meet the objectives described above and should not be used for other purposes.

Finally, while we distributed this report in draft to management under the title of “Independent Evaluation of EEOC Privacy Program,” we noted during our quality control process that the wording “independent audit,” not “evaluation,” should have been used. We therefore have changed the wording from independent evaluation to independent audit in several places in the report.

We appreciate the opportunity to have worked with EEOC. Please call me if you have questions.

Very truly yours,
COTTON & COMPANY LLP

Loren F. Schwartz, CPA, CISA, CIPP
Partner

INTRODUCTION

The Equal Employment Opportunity Commission (EEOC or Commission), Office of Inspector General (OIG) contracted with Cotton & Company LLP to conduct an audit of privacy and data protection policies, procedures, and practices. We reviewed EEOC's privacy related controls from May 28, 2008, through July 31, 2008. Such a review had not been previously performed by the EEOC OIG. Testing was primarily focused on requirements from federal laws and regulations, as well as from best practices in the field of privacy.

BACKGROUND

Equal Employment Opportunity Commission

EEOC was created by Title VII of the Civil Rights Act of 1964, but its mission has been shaped by more than this one piece of legislation. Numerous laws and amendments and a handful of executive orders have expanded, limited, or directed EEOC's responsibilities and authority.

EEOC has five Commissioners and a General Counsel, appointed by the President and confirmed by the Senate. The Commissioners make equal employment opportunity policy and approve most litigation. Commissioners are appointed for five-year, staggered terms, and the General Counsel has a four-year term. The President designates a Chair, who is also the Chief Executive Officer, and a Vice Chair.

The EEOC's Office of Legal Counsel (OLC) serves as the principal advisor to the Commission on enforcement matters. OLC represents the Commission in defensive litigation and administrative hearings, and prepares Commission decisions on charges for which there is no precedent. OLC writes regulations, conducts outreach and education efforts, and coordinates all federal issues affecting equal employment opportunity. EEOC's Legal Counsel is assigned with Senior Agency Official for Privacy (SAOP) responsibilities.

EEOC is headquartered in Washington D.C. with 53 field offices distributed across the country. EEOC has offices in 32 states.

Federal Privacy Framework

The purpose of the Privacy Act of 1974 is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to:

- Permit an individual to determine what records pertaining to him/her are collected, maintained, used, or disseminated by such agencies;
- Permit an individual to prevent records pertaining to him/her obtained by such agencies for a particular purpose, from being used or made available for another purpose without consent;
- Permit an individual to gain access to information pertaining to him/her in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records; and

- Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

OBJECTIVES, SCOPE, AND METHODOLOGY

Cotton & Company conducted an independent audit of EEOC's privacy and data protection policies and procedures to assess the effectiveness of EEOC's identification of sensitive personally identifiable information (PII) that is collected, processed, and stored within the EEOC. We assessed EEOC's documented privacy policies and procedures; and we analyzed EEOC's intranet, network, and websites for privacy vulnerabilities, including noncompliance with stated policies, practices, and procedures, and risks for inadvertent release of information in an identifiable form from the website.

We conducted our audit of EEOC's privacy and data protection policies, procedures, and practices in three phases: Planning, Testing, and Reporting.

Cotton & Company begins all engagements with a planning phase, where we gain and update our understanding of EEOC and its mission, types of activities and information used, and practices and procedures to ensure that EEOC's mission can be accomplished. We use our understanding to refine our scope and specific audit steps to ensure that we meet overall objectives.

During the planning phase we focused on three areas: 1) reviewing privacy-governance-related documentation and audit reports; 2) conducting preliminary meetings with key management and operational personnel responsible for creating and implementing privacy protection practices and monitoring compliance with legislation; and 3) conducting a cross-functional privacy survey.

The testing phase resulted in an assessment of EEOC's controls over use and protection of PII. Cotton & Company developed specific testing procedures to conduct privacy audits of federal agencies. These procedures helped determine if PII had been adequately identified and sufficient controls had been put in place to restrict access.

At the conclusion of testing, we created a written report detailing our analysis of EEOC's effectiveness in identifying and protecting PII and included recommendations for correcting identified weaknesses.

This audit followed standards as promulgated by the Yellow Book, *Government Auditing Standards* (2007 Revision). Fieldwork was completed on July 31, 2008.

SUMMARY OF RESULTS

Overall, we believe EEOC is substantially meeting privacy related requirements set forth by Congress, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Specific areas where the EEOC addresses privacy requirements include:

- Conducting privacy impact assessments in compliance with Section 208 of the E-Government Act;
- Developing and delivering privacy related training to EEOC employees and contractors;
- Maintaining a System of Records Notice, in accordance with the 1974 Privacy Act; and
- Developing privacy incident response policies and procedures in accordance with OMB guidance.

However, we identified specific areas where privacy policies, procedures, and practices could be strengthened. We provided management with our findings and recommendations for comment. Management comments have been incorporated into this report. See the Appendix for management comments in their entirety. Weaknesses identified during our audit are noted below.

DETAILED FINDINGS AND RECOMMENDATIONS

Finding 1: EEOC Has Not Developed Safeguards over Hard Copy Sensitive Personally Identifiable Information (PII)

Controls were not adequate to ensure that EEOC adequately protected hard copy documentation containing sensitive PII at headquarters and field offices. Specifically, we found numerous instances of unprotected documentation containing sensitive PII during after hours walkthroughs of the EEOC Headquarters and the Baltimore Field Office including:

- Case files containing PII, such as full name, home address, date of birth, social security number, medical disability information, and employment records in unlocked cabinets, in drop-boxes on desks, and in unlocked boxes waiting to be disposed of, in open common areas;
- Official TDY Traveler Authorization and Travel Voucher forms containing names, social security numbers, and home addresses of EEOC employees, unsecured on desks;
- Government Bill of Lading files containing names, addresses, and social security numbers;
- Payroll documents on cubicle desks, containing names, office IDs, and social security numbers;
- Stacks of EEOC Personnel Files containing employee names, addresses, dates of birth, social security numbers, and signatures in hallway filing cabinets;
- Completed W-4 tax forms; and
- Unlocked doors, including the main door on the second floor, which allows entry from the elevators to the Washington Field Office (WFO), as well as the door that allows entry from the WFO into the Office of the Chief Financial Officer; allowing anyone with building access, entry to any unsecured information on that floor.

EEOC Order 240.005, Appendix A, *Information Security Responsibilities of EEOC System Users*, dated May 2007, states:

Section 7, *Accountability and Control Responsibilities*:

EEOC System users are responsible for ensuring the security of sensitive information and protecting the technology and equipment which supports its information systems as specified in the following:

g) System users must take appropriate measures to secure paper reports containing sensitive information and properly dispose of these materials through shredding or other appropriate means.

Section 8, *Other EEOC System User Information Security Responsibilities*:

Take appropriate measures to secure (i.e., protect from unauthorized or illegal disclosure or alteration) and dispose of (i.e., shred) printouts containing sensitive information.

EEOC's *Policy for Personally Identifiable Data Extracts Removed from EEOC Premises*, dated October 2006, Section IV, *Roles and Responsibilities*, page 2 states:

Information owners are responsible for protection of their data.

OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, dated May 22, 2006, page 1, states:

This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area.

While EEOC has annual security awareness and privacy training in place, which notifies employees and contractors of their responsibilities for protecting PII, we believe controls could be strengthened by providing all employees and contractors with periodic reminders of their responsibilities. Because security awareness and privacy training are provided once a year, the likelihood of individuals relaxing their practices in protecting sensitive PII increases without periodic reminders.

Finally, we noted that EEOC does not have specific controls in place (such as periodic physical walkthroughs of work areas) to ensure that employees are adequately protecting sensitive PII in their possession. By not securing hard copy documents within offices, a potential breach of PII is possible by anyone in the building during and after hours, including malicious employees, cleaning crew, or security personnel.

Recommendations

We recommend that the SAOP:

1. Develop and implement policies and procedures to provide periodic (more frequent than annual) reminders, to all employees and contractors, of their responsibilities to protect sensitive PII in both electronic and hard copy format.
2. Develop, document, and implement procedures to monitor compliance with EEOC policies and procedures related to the protection, processing, storage, and destruction of sensitive hard copy PII.

Management Response:

SAOP Response: SAOP concurs with the finding and recommendations.

OIT Response: OIT concurs with the finding and recommendations.

ORIP Response: No comment.

Auditor Response: OIG concurs.

Finding 2: EEOC Website Privacy Policies Are Incomplete and Inconsistently Applied

Controls were not adequate to ensure that EEOC had developed and posted privacy policies to their website, in accordance with OMB regulations. Specifically, we found that privacy policies posted to the following websites did not contain all information required by OMB:

- www.eeoc.gov (Main EEOC Website)
- www.youth.eeoc.gov (Youth at Work) (Subdomain of www.eeoc.gov)
- https://apps.eeoc.gov/eas/ (EEOC Assessment System Webpage) (Subdomain of www.eeoc.gov)

In particular, the following items were missing from all privacy policies, as required by OMB:

- Consent to collection and sharing;
- Rights under the Privacy Act, Privacy Act information and statements;
- Use of web bugs/beacons;
- Automatically collected information (EEOC Assessment System Webpage only);
- Security of information collected (Main Website and Youth at Work websites only); and
- Law enforcement sharing.

In addition, while OMB requires that a privacy policy be posted to all web pages that collect information, the following EEOC web pages were not in compliance with this requirement:

- http://www.eeotraining.eeoc.gov (Training Website) (Subdomain of www.eeoc.gov)
- http://eeoc.gov/eeo1survey/index.html (EEO-1 Survey)
- http://www.eeoc.gov/federal/form462/index.html (Form 462)
- http://eeoc.gov/publications.html (Publication Requests)
- https://www.eeotraining.eeoc.gov/profile/form/index.cfm

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the EGovernment Act of 2002*, September 26, 2003, states:

Section III D

Content of Privacy Policies.

1. *Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:*
    - *Consent to collection and sharing; and*
    - *Rights under the Privacy Act or other privacy laws.*
2. *Agency Privacy Policies must continue to address the following, modified, requirements:*
    - *Privacy Act information;*
    - *Privacy Act Statements;*
    - *Automatically Collected Information (site management data);*
    - *Tracking and customization activities; and*
    - *Security of the information.*

Section III E

Placement of Notices. Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:

- *Their principal web site;*
- *Any known, major entry points to their sites; and*
- *Any web page that collects substantial information in identifiable form.*

Administration of EEOC's websites is not centrally managed. Units may control their own websites, causing inconsistencies and/or incompleteness in privacy policies.

Without adequate privacy policies posted on websites, customers visiting EEOC websites are not made fully aware of EEOC policies.

Recommendations

We recommend that the SAOP:

1. Centralize administration of website privacy policies.
2. Ensure that all privacy policies posted to EEOC websites comply with OMB requirements.
3. Ensure that privacy policies are posted on:
    a. EEOC's principal website.
    b. Any known, major entry points to EEOC sites.
    c. Any web page that collects substantial information in identifiable form.

Management Response:

SAOP Response: SAOP concurs with the finding and recommendations.

OIT Response: OIT concurs with the finding and recommendations.

ORIP Response: No comment.

Auditor Response: OIG concurs.

Finding 3: EEOC Has Not Identified and Documented Applicable Privacy Laws and Regulations

Controls were not adequate to ensure that EEOC had identified and documented specific privacy laws and regulations that pertain to the organization. The SAOP stated that a documented review of which privacy related laws and regulations are applicable to EEOC, has not been performed, and that EEOC adheres to all privacy laws except for ones that specify a Chief Privacy Officer. The SAOP has not made it a priority to review and document all relevant privacy laws and regulations to identify which ones are applicable to EEOC.

OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, dated February 11, 2002, page 1, states:

The senior agency official will have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

Agencies are required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies.

By not identifying applicable privacy laws, EEOC may not be able to implement the controls required to address potential privacy risks.

Recommendations

We recommend that the SAOP:

1. Review all privacy laws and regulations, and identify and document those applicable to EEOC.
2. Develop, document, and implement a formal process for ensuring all new privacy related laws and regulations are evaluated to determine whether the EEOC is required to follow them.

Management Response:

SAOP Response: SAOP disagrees with this finding and believes they have identified privacy laws and regulations applicable to EEOC. SAOP concurs that they have not documented what privacy laws and regulations are applicable to EEOC.

OIT Response: No comment.

ORIP Response: No comment.

Auditor Response: We continue to believe the SAOP has not identified and documented what privacy laws and regulations are applicable to EEOC. The lack of a formalized process for identifying applicable laws and regulations and documenting their applicability increases the risk that EEOC may not comply with applicable privacy laws and regulations. We continue to recommend that the SAOP review all privacy laws and regulations and identify and document those which are applicable to EEOC. Additionally, we continue to recommend that the SAOP develop, document, and implement a formal process for ensuring all new privacy related laws and regulations are evaluated to determine whether EEOC is required to follow them.

Finding 4: EEOC Has Not Implemented Two-Factor Authentication

Controls were not adequate to ensure that EEOC had implemented technologies to help ensure that privacy information is adequately secured from unauthorized use or disclosure. Specifically, we found that EEOC does not utilize two-factor authentication for remote VPN access, as defined by OMB Memorandum M-06-16. Currently, EEOC identifies the computer network login username and password, and the separate VPN login username and password as two-factor authentication.

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, page 1, states:

The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote information. The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:

1. *Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.*

EEOC has not yet implemented two-factor authentication for remote VPN access to the network because it is waiting to implement a Homeland Security Presidential Directive (HSPD) – 12 compliant smart card badge system.

Because EEOC does not have two-factor authentication for remote VPN access, the likelihood that an unauthorized user may be able to access the EEOC network remotely with access to an employee's laptop and login credentials is increased, which can lead to a loss or breach of sensitive information.

Recommendations

We recommend that the SAOP continue with the planned action to implement two-factor authentication with the implementation of HSPD-12 badges. Until this weakness is resolved, management should continue to include this weakness in their Plan of Action and Milestones (POAM).

Management Response:

SAOP Response: SAOP concurs with comments submitted by OIT.

OIT Response: In the text describing the finding, it is stated that, "Currently, EEOC identifies the computer network login username and password, and the separate VPN login username and password as two-factor authentication." OIT seeks to clarify this misstatement. EEOC understands that separate logins ("something you know") does not provide two-factor authentication (something you know and something you have), however we have implemented multiple compensating controls to mitigate this risk. These compensating controls include:

1) Hardware-based "boot-up" password on all EEOC laptops;
2) User specific Windows login/password to access laptop applications;
3) Separate user specific VPN login/password; and
4) Once connected to VPN, entry of EEOC user-specific network login/password.

These four layers of password control are on three separate devices, and while we understand that this does not constitute "two-factor authentication," the compensating controls have lowered the risk to an acceptable level, per CIO concurrence, until two-factor authentication is implemented via our new Fed ID Homeland Security Presidential Directive #12 (HSPD-12) program.

As a small agency, EEOC cannot afford the monetary, human, and time resources that would be required to acquire, implement/configure, train users, and manage an enterprise-wide token-based solution that would be in use for less than 12-months from time of deployment. Resources are currently being expended toward implementing new Personal Identity Verification (PIV2)-compliant Federal IDs for all employees/system users, acquiring new laptops with embedded PIV2 card readers (timed to coincide with laptop lease renewals in late FY 2009), and integrating these cards/readers with VPN authentication (FY 2010). EEOC cannot afford to acquire, implement, and manage two separate token-based systems concurrently: one for short-time use and one for long-term use. Since the new FED IDs can be used for both building access and system access, it is not efficient to require employees to carry their FED ID and a separate token device. The acceptance of this risk and the current approved plan of action have been outlined in appropriate System Security Plans and OMB POAM reports.

ORIP Response: No comment.

Auditor Response: The OIG notes that OIT agrees with the finding, has implemented compensating controls where possible and accepts the remaining risk until this weakness can be properly resolved. Until this weakness is resolved management should continue to include this weakness in their POAM.

AUDIT FOLLOW-UP

OMB issued Circular Number A-50, *Audit Follow-Up*, to ensure that corrective action on audit findings and recommendations proceed as rapidly as possible. EEOC Order 192.002, *Audit Follow-Up Program*, implements Circular Number A-50 and requires that for resolved recommendations, a corrective action work plan should be submitted within 30 days of the final audit report date describing specific tasks and indicating the completion dates necessary to implement audit recommendations. Circular Number A-50 requires prompt resolution and corrective action on audit recommendations. Resolutions should be made within six months of final report issuance.

APPENDIX
MANAGEMENT RESPONSES

September 18, 2008

MEMORANDUM

TO: Aletha L. Brown, Inspector General

FROM :Reed L. Russell
Senior Agency Official for Privacy/Legal Counsel

SUBJECT:Report on FY08 Evaluation of EEOC Privacy Program

We have reviewed draft audit report # 08-12-AEP prepared by Cotton & Co. and are pleased that the auditors found that "EEOC is substantially meeting privacy related requirements set forth by Congress, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST)." P.2. Below are comments on the specific areas where the auditors found that policies, practices and procedures could be strengthened.

Finding 1: EEOC Has Not Developed Safeguards Over Hard Copy Sensitive Personally Identifiable Information (PII).

We agree that more can be done in this area. We will consider appropriate mechanisms to provide periodic reminders throughout the year to employees of their information security obligations with respect to hard copy and electronic PII as well as appropriate monitoring procedures to detect noncompliance.

Finding 2: EEOC Website Privacy Policies are Incomplete and Inconsistently Applied.

We agree that the existing Privacy Policies should be reviewed for consistency and compliance with applicable requirements and that responsibility for website privacy policies should be centralized.

Finding 3: EEOC Has Not Identified and Documented Applicable Privacy Laws and Regulations.

We disagree with the part of the finding stating that EEOC has not identified the privacy laws and regulations that pertain to EEOC. We believe that we are aware of, and in compliance with, all such applicable laws and regulations. The draft report does not identify any law or regulation applicable to EEOC of which we were unaware. To the extent that the finding focuses on documenting the identification of such laws and regulations, we agree that we have not compiled a list of all such laws and regulations but question whether compilation of such a list is necessary. We will inquire with other agencies to determine how they handle the documentation requirement in OMB Memo M-05-08.

Finding 4: EEOC Has Not Implemented Two-Factor Authentication.

We concur in the comments on this item previously submitted by CIO Kimberly Hancher.

cc: Anthony Kaminski
Kimberly Hancher
Deidre Flippen

MEMORANDUM

TO: Aletha L. Brown, Inspector General

FROM :Kimberly Hancher sent via email 9/9/2008
Chief Information Officer

SUBJECT:OIT Comments on FY08 Evaluation of EEOC Privacy Program; Report # 08-12-AEP

Thank you for the opportunity to review the above referenced Privacy Program Report. Below are the Office of Information Technology's (OIT) comments on the draft findings and recommendations:

Finding 1: EEOC Has Not Developed Safeguards Over Hard Copy Sensitive Personally Identifiable Information (PII).

Recommendations:

1. **Develop and implement policies and procedures to provide periodic (more frequent than annual) reminders, to all employees and contractors, of their responsibilities to protect sensitive PII in both electronic and hard copy format.**

   OIT will work with the Office of Legal Counsel (OLC) to augment Security Awareness Training program to include periodic PII reminders.

2. **Develop, document, and implement procedures to monitor compliance with EEOC policies and procedures related to the protection, processing, storage, and destruction of sensitive hard copy PII.**

   OIT will assist the OLC by reviewing new draft policies and procedures.

Finding 2: EEOC Website Privacy Policies are Incomplete and Inconsistently Applied.
Recommendations:

1. **Centralize administration of website privacy policies.**
2. **Ensure that all privacy policies posted to EEOC websites comply with OMB requirements.**
3. **Ensure that privacy policies are posted on:**
   a. **EEOC's principal web site.**
   b. **Any known, major entry points to EEOC sites.**
   c. **Any web page that collects substantial information in identifiable form.**

   OIT concurs and will develop and post policy for the EEO-1 and EAS as outlined in the finding.

Finding 3: EEOC Has Not Identified and Documented Applicable Privacy Laws and Regulations

No comment.

Finding 4: EEOC Has Not Implemented Two-Factor Authentication

Recommendation:

We recommend that the SAOP utilize token devices to establish two-factor authentication for remote VPN access until the smart card badge system is fully implemented and functional.

In the text describing the finding, it is stated that, "Currently, EEOC identifies the computer network login username and password, and the separate VPN login username and password as two-factor authentication." OIT seeks to clarify this misstatement. EEOC understands that

separate logins ("something you know") does not provide two-factor authentication (something you know and something you have), however we have implemented multiple compensating controls to mitigate this risk. These compensating controls include:

1. Hardware-based "boot-up" password on all EEOC laptops;
2. User specific Windows login/password to access laptop applications;
3. Separate user specific VPN login/password; and
4. Once connected to VPN, entry of EEOC user-specific network login/password.

These four layers of password control are on three separate devices, and while we understand that this does not constitute gtwo-factor authentication,h the compensating controls have lowered the risk to an acceptable level, per CIO concurrence, until two-factor authentication is implemented via our new Fed ID Homeland Security Presidential Directive #12 (HSPD-12) program.

As a small agency, EEOC cannot afford the monetary, human, and time resources that would be required to acquire, implement/configure, train users, and manage an enterprise-wide token-based solution that would be in use for less than 12-months from time of deployment. Resources are currently being expended toward implementing new Personal Identity Verification (PIV2)-compliant Federal IDs for all employees/system users, acquiring new laptops with embedded PIV2 card readers (timed to coincide with laptop lease renewals in late FY 2009), and integrating these cards/readers with VPN authentication (FY 2010). EEOC cannot afford to acquire, implement and manage two separate token-based systems concurrently: one for short-time use and one for long-term use. Since the new FED IDs can be used for both building access and system access, it is not efficient to require employees to carry their FED ID and a separate token device. The acceptance of this risk and the current approved plan of action have been outlined in appropriate System Security Plans and OMB POAM reports.

cc: Anthony Kaminski
Reed Russell
Deidre Flippen

From: JAY FRIEDMAN
To: GENERAL, INSPECTOR
Date: Mon, Sep 8, 2008 12:36 PM
Subject: Re: Draft Report:FY2008 Evaluation of the EEOC's Privacy Program

Deidre:

I have no comments on Cotton's report.

Jay