U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Quick Reaction Report

Identification Proofing, Incident Handling, and Badge Disposal Procedures Needed for EPA's Smartcard Program

Report No. 08-P-0267

September 16, 2008

Report Contributors: Rudolph M. Brevard
Corey Costango
Neven Morcos

Abbreviations

EPA	U.S. Environmental Protection Agency
EPASS	EPA Personnel Access and Security System
FIPS	Federal Information Processing Standards
HSPD-12	Homeland Security Presidential Directive 12
ID	Identification
OASIS	Office of Administration Services Information System
OIG	Office of Inspector General
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SMD	Security Management Division

U.S. Environmental Protection Agency
Office of Inspector General

08-P-0267
September 16, 2008

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Office of Inspector General performed this review in response to an inquiry related to controls over identification documents used for issuing the new U.S. Environmental Protection Agency (EPA) Smartcard badges. We performed this review as a result of a specific incident. We conducted a limited review of EPA's policies and procedures for processing identification information collected, responding to Smartcard badge incidents, and handling of defective Smartcards.

Background

Homeland Security Presidential Directive 12 established the requirements for a common standard for identifying credentials issued by federal departments and agencies to federal employees and contractors. EPA instituted the EPA Personnel Access and Security System (EPASS) program to satisfy this Directive. The program is part of EPA's larger effort to create an integrated system to safeguard and manage workforce identity, facility access, and computer system access throughout EPA.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:
www.epa.gov/oig/reports/2008/20080916-08-P-0267.pdf

Identification Proofing, Incident Handling, and Badge Disposal Procedures Needed for EPA's Smartcard Program

What We Found

Although EPA developed detailed procedures to guide the EPASS staff's issuance of new Smartcard identification (ID) badges, an employee error in using the new ID card system resulted in an EPA employee having ID documents and other identifying information incorrectly associated with another EPA employee. An EPASS employee incorrectly accessed the wrong employee's computer record, scanned the ID documents for the employee requesting the Smartcard, then associated the scanned documents with the incorrectly accessed computer record. Also, EPA's procedures for issuing ID cards lacked a vital step required by federal guidance. In particular, EPA procedures did not require EPASS staff to visually inspect ID documents and compare them against the individual requesting the Smartcard and the name on the accessed computer record.

Although we did not discover more than one incident, we found that EPA lacks procedures to ensure employees take steps to correct similar incidents when they occur. Further, EPA lacks procedures for handling and disposing of defective Smartcard badges that contain personally identifiable information. According to Security Management Division managers, documenting procedures has been delayed because management attention has been focused on meeting the Office of Management and Budget deadline to roll out the EPASS program.

Authenticating an individual's identity is a critical factor for controlling physical and logical access to EPA resources. Without taking immediate steps to correct the weaknesses noted, doubts will exist over whether EPA has the ability to become a trusted agent for verifying ID credentials as federal agencies integrate their Smartcard programs.

What We Recommend

We recommend that the Director, Security Management Division, Office of Administration and Resources Management:

- Update existing identification card issuing procedures to ensure the procedures include all mandatory steps.
- Create incident-handling procedures to be used by EPASS program staff when errors in the ID card issuing process occur.
- Create and implement procedures for proper handling and disposal of defective ID badges.

The Agency agreed to implement our recommendations, and we consider the actions planned to be satisfactory.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

September 16, 2008

MEMORANDUM

SUBJECT: Identification Proofing, Incident Handling, and Badge Disposal Procedures Needed for EPA's Smartcard Program
Report No. 08-P-0267

FROM: Patricia H. Hill
Assistant Inspector General for Mission Systems

TO: Wes Carpenter
Director, Security Management Division
Office of Administration and Resources Management

This report contains time-critical issues the Office of Inspector General (OIG) identified. This report represents the opinion of the OIG and does not necessarily represent the final position of the U.S. Environmental Protection Agency (EPA). EPA managers will make final determinations on matters in this report.

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $120,287.

Action Required

The Office of Administration and Resources Management does not have to provide a response to this report. The Agency's response to the draft report contained an adequate corrective action plan with milestone dates to implement the plan. Accordingly, we are closing this report on issuance. We have no objection to further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0893 or brevard.rudy@epa.gov. You may also contact Neven Morcos or Corey Costango, Project Managers, at (202) 566-9688 or (202) 566-2552, respectively.

Table of Contents

Appendices

Purpose

The Office of Inspector General (OIG) initiated this review in response to an inquiry regarding the controls over identification (ID) documents used for issuing the new Smartcard badges. We initiated this review after an incident in which an U.S. Environmental Protection Agency (EPA) employee went to pick up a Smartcard badge and the badge contained the employee's name but another employee's image. We conducted a limited review of EPA's policies and procedures for processing ID information. We reviewed how EPA responds to Smartcard badge incidents and how EPA handles defective Smartcard badges.

Background

Homeland Security Presidential Directive 12 (HSPD-12) established the requirements for a common ID standard for ID credentials issued by federal departments and agencies. HSPD-12 directed the Department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common ID credential that became FIPS 201. FIPS 201 specifies a Personal Identity Verification (PIV) system through which common ID credentials can be created and later used to verify a claimed identity. The EPA Personnel Access and Security System (EPASS) Smartcard badge and the associated management program have been instituted to satisfy EPA's compliance with HSPD-12 and FIPS 201. The EPASS program is part of EPA's larger effort to create an integrated system to safeguard and manage workforce identity, physical access, and logical access throughout the Agency. EPA's Security Management Division (SMD), in the Office of Administration and Resources Management, is responsible for managing the EPASS program in compliance with all applicable authorities and directives.

Operation of the Agency's EPASS program is outlined in two key procedure documents – the PIV Handbook and the EPASS Operation Manual. The PIV Handbook establishes EPA's standard operating procedures for EPASS. The EPASS manual is designed to be a training document for EPASS registrars and issuers. The manual provides step-by-step descriptions for the Agency's ID proofing, enrollment, and badge issuance processes. During ID proofing, the registrar should:

1. Verify the applicant's sponsorship status in the Office of Administration Services Information System (OASIS). OASIS is the authoritative source for EPASS badge holder identity information and maintains the demographic data (name, individual affiliation, etc.) needed to initiate a request.

2. Select and copy the applicant's name from OASIS into another application called Identix. Identix is an application used during enrollment to collect an applicant's demographic data, fingerprints, and photograph.

3. Verify the authenticity of the presented ID documents and that they prove the identity of the applicant.

The enrollment process is where the applicant's demographic data, fingerprints, and photograph are collected. During badge issuance, the issuer allows the applicant to personalize the badge with a personal ID number. The issuer also has the applicant perform a fingerprint check for verification. The Agency's new Smartcard ID badge contains Personally Identifiable Information (PII) such as an employee's name, photograph, and fingerprint data. However, the Agency indicated that the Smartcard ID badge does not contain a Social Security number or comparable identification numbers, which would be considered Sensitive PII according to EPA's Privacy Policy.

Scope and Methodology

We conducted this audit from April through July 2008 at EPA Headquarters in Washington, DC, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

We evaluated the management control processes over EPA's Smartcard ID proofing and badge issuance processes. We reviewed the Agency's EPASS program procedures. We interviewed EPA staff responsible for overseeing the EPASS program, and EPA contractors responsible for the daily operations of EPASS. We had not performed prior reviews/audits related to EPA's Smartcard ID proofing and badge issuance processes, so there were no recommendations to follow up on during this audit.

Findings

Although EPA developed sufficient Smartcard ID card issuance procedures, we found that an employee error in using the new ID card system led to an EPA employee having ID documents associated with another EPA employee. An EPASS system operator accessed the wrong employee's computer record, scanned the ID documents for the employee requesting the new ID card, then associated the scanned documents with the incorrectly accessed computer record. Also, EPA's ID card issuing procedures lacked a vital step required by federal guidance. In particular, EPA procedures do not require ID proofing staff to visually inspect collected ID documents and compare them to the individual requesting the new ID card and the name of the computer record that is accessed.

Although we did not discover more than this incident, we found that EPA lacks procedures to ensure that if similar incidents happen again, steps are taken to correct them in a consistent manner. Further, EPA lacks procedures for handling and destroying defective ID card badges that contain individuals' ID information.

SMD managers indicated that procedures have not been documented because they have focused on meeting the Office of Management and Budget's deadline for rolling out the EPASS program. Maintaining control of defective Smartcard ID badges until they are properly disposed of is important because data on the Smartcard ID badges is PII. The Federal Government's Smartcard program is built on a chain of trust that starts with the proper verification of a card applicant's

identity. ID badges are going to be uniform government-wide and will eventually be used to access any Federal agency. Implementing these badges across the government will make each agency more individually accountable for the overall physical security of the Federal Government.

EPASS Procedures Need Updating to Include All Federal Requirements

EPASS program procedure documents are missing a key step in verifying a card applicant's identity, which contributed to the ID badge incident. According to FIPS 201, when verifying a card applicant's identity:

1. "The PIV Registrar shall visually inspect the identification documents and authenticate them as being genuine and unaltered;

2. "…verify the authenticity of the source document; and

3. "…compare the picture on the source document with the Applicant to confirm that the Applicant is the holder of the identity source document."

Neither the PIV Handbook nor EPASS Operation Manual – which describe EPASS procedures for ID proofing, enrollment, and badge issuance – includes a step for visually inspecting proof of identity documents and comparing them to the applicant as part of the ID proofing process.

The current ID proofing procedures contain steps that should have allowed EPASS staff to recognize the mistake made during the ID proofing process. According to the EPASS Operation Manual, during ID proofing and enrollment, an applicant is supposed to present a valid ID before each process starts. At the beginning of ID proofing, the applicant presents a form of identification. The applicant's name is then selected from OASIS and copied into Identix. Before the next step (enrollment) starts, an applicant is supposed to present their identification again and additional data is entered into Identix. The aforementioned ID proofing procedures were additional opportunities that should have allowed the registrar or issuer to determine that they selected the wrong EPA employee.

Procedures Needed for Handling Smartcard Incidents

EPASS program managers had not developed internal procedures to handle errors in the Smartcard issuance process. When EPASS program managers were alerted of the ID badge incident, they sought to resolve and correct the problem. EPASS managers discovered that the source of the problem was in ID proofing. The two employees involved in the incident have similar last names. After collecting the sensitive employee authentication data the data was mistakenly saved under the wrong employee's name. To correct this problem, EPASS managers instructed the system administrator to move and delete the sensitive employee authentication data from the wrong employee's record and copy it into the correct employee's record, which circumvented EPASS ID proofing procedures.

EPASS program representatives indicated this was the first time this type of situation occurred. Also, they indicated that the security controls built into the Smartcard issuance process prevented the card from being issued. However, during our review, the EPASS staff could not provide us with documentation that supported how they corrected the incident in question. This documentation would include what steps the EPASS staff took and when EPA management was informed about the incident

Having documented procedures and records is important because they provide the framework for ensuring EPASS staff consistently follow steps prescribed by EPA management. Further, the new EPA Smartcard contains an employee's PII. Having documented procedures would allow EPASS staff to respond to a PII incident as required by EPA's "Personally Identifiable Information (PII) Incident Handling & Response Procedure." This Procedure requires program managers to tailor incident response activities to meet their specific security or business requirements. However, EPASS program managers had not developed internal PII incident response procedures

We found that EPASS program managers had not established procedures to monitor system administrator changes to employee's ID records. To resolve this incident, EPASS program managers corrected the problem by having the system administrator copy, delete, and move data within the system. These types of system changes bypass the established workflow processes that ensure the accurate verification of ID credentials and accurate association of these credentials with the right individual. EPASS program representatives informed us that changes within the system are recorded in the system audit logs. However, these logs are currently not being reviewed.

Procedures Needed for Handling Defective Badges

The EPASS program does not have procedures for handling and disposing of defective Smartcard badges. Since the badge of concern contained one employee's name and another's picture and fingerprint data, we sought to determine the status of the Smartcard badge in question. Program representatives informed us they had the badge locked in a safe until the EPASS staff was sure it was appropriate to dispose of it. We asked the program representatives if these were their usual procedures for handling similar incidents. They informed us they did not have formal procedures in place because this defective badge incident was a one-time occurrence. Although one case does not sound significant, in the context of employee ID proofing and issuance, one incident could undermine the confidence individuals place in EPA's ability to protect their confidentially provided PII.

During the course of interviews, we discovered another instance where the EPASS staff cannot issue Smartcard badges as intended. According to EPASS representatives, when personnel come to pick up their ID badges they must create a personal ID number and provide a fingerprint check for verification. EPASS program representatives stated it was common for a number of badges to not work during the fingerprint verification process. If the card did not pass the fingerprint verification process, the EPASS staff would not issue the defective card and would replace it with a new one. At this point in the ID issuance process, these defective badges contain the

individual's name, picture, and fingerprint data. Therefore, procedures for handling, storing, and disposing of these defective Smartcard badges are important in order to secure the PII on them.

Recommendations

We recommend that the Director, Security Management Division, Office of Administration and Resources Management:

1. Update existing ID card issuing procedures to ensure the procedures include all mandatory steps required by FIPS 201. This should include steps to require EPASS program staff to visually inspect ID documents for proper verification of the applicant's identity.

2. Create incident-handling procedures to be used by EPASS program staff for recording, resolving, and notifying management when errors in the ID card issuing process occur. These procedures should include adopting, where applicable, EPA's "Personally Identifiable Information (PII) Incident Handling & Response Procedure." These procedures should also include the processes EPASS staff should use to correct employee records in the EPASS system, note how the changes to system records should be documented, and define a process for reviewing modified employee records for authorized changes.

3. Create and implement procedures for the proper handling and disposing of defective ID badges.

Agency Comments and OIG Response

The Agency concurred with the report's recommendations and provided a corrective action plan to address them. We believe the Agency's planned actions, once completed, would adequately address the report's recommendations. However, the Agency requested that we modify the report to clarify the type of PII and fingerprint data that is stored on the new EPASS badges. The Agency also requested that we modify one sentence in the report that inferred the ID card incident in question was the result of a wrongfully issued EPASS badge. We reviewed the Agency comments and, where appropriate, modified the report to use consistent language regarding information stored on EPASS badges and the causes for the ID card incident in question. The Agency's complete response is at Appendix A.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	5	Update existing ID card issuing procedures to ensure the procedures include all mandatory steps required by FIPS 201. This should include steps to require EPASS program staff to visually inspect ID documents for proper verification of the applicant's identity.	O	Director, Security Management Division, Office of Administration and Resources Management	10/15/2008		
2	5	Create incident-handling procedures to be used by EPASS program staff for recording, resolving, and notifying management when errors in the ID card issuing process occur. These procedures should include adopting, where applicable, EPA's "Personally Identifiable Information (PII) Incident Handling & Response Procedure." These procedures should also include the processes EPASS staff should use to correct employee records in the EPASS system, note how the changes to system records should be documented, and define a process for reviewing modified employee records for authorized changes.	O	Director, Security Management Division, Office of Administration and Resources Management	12/15/2008		
3	5	Create and implement procedures for the proper handling and disposing of defective ID badges.	O	Director, Security Management Division, Office of Administration and Resources Management	12/15/2008		

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Agency's Response to Discussion Draft Report

MEMORANDUM

SUBJECT: Response to Quick Reaction Report Discussion Draft

FROM: Renee Page, Director /s/
Office of Administration

TO: Rudolph M. Brevard, Director
Information Resources Management Assessments
Office of Inspector General

Thank you for the opportunity to comment on the Office of Inspector General's (OIG's) Quick Reaction Report Discussion Draft of July 11, 2008: *Identification Proofing, Incident Handling, and Badge Disposal Procedures Needed for EPA's Smartcard Program.*

The Security Management Division (SMD) concurs with the Report's three recommendations. Our implementation plans and associated milestones are below.

Our only comments are to clarify the issue of Personally Identifiable Information (PII) on the EPASS badge. The Report states, "…data on the Smartcard ID badges is Personally Identifiable Information" (p. 2); badges "…contain individuals' ID information" (p. 2); and "…the new EPA Smartcard contains an employee's PII" (p.4). Please note that the only PII displayed or stored on the badge is the employee's name and photograph. The badge does not contain a Social Security number or other information considered sensitive PII, as defined by the Agency's Privacy Policy (http://www.epa.gov/privacy/policy/2151/index.htm).

The report also states that badges contain individuals' fingerprints (p. 4). The badge does not contain fingerprints, but rather a fingerprint template, a mathematical representation of certain minutiae (see attached file). The template cannot be used to construct a fingerprint image.

Finally, we respectfully request the deletion or correction of one sentence: "We reviewed how EPA responds to incidents of wrongfully issued Smartcard badges" (p. 1). The incident in question and the Quick Reaction Review did not involve a wrongfully issued badge. The Report itself states "…the security controls built into the Smartcard issuance process prevented the card from being issued" (p. 3) and "…we did not discover more than the one incident" ("At a Glance" page).

The following is SMD's corrective action plan to implement OIG's recommendations:

1. *Update existing ID card issuing procedures to ensure the procedures include all mandatory steps required by FIPS 201. This should include steps to require EPASS program staff to visually inspect ID documents for proper verification of the applicant's identity.*

   SMD will update procedures to require EPASS staff to visually inspect identity documents and ensure a match between any photograph and the EPASS applicant, and between the name on identity documents and the name in the EPASS record. Implementation milestone: Updated procedures will be in place by October 15, 2008.

2. *Create incident-handling procedures to be used by EPASS program staff for recording, resolving, and notifying management when errors in the ID card issuing process occur. These procedures should include adopting, where applicable, EPA's "Personally Identifiable Information (PII) Incident Handling & Response Procedure." These procedures should also include the processes EPASS staff should use to correct employee records in the EPASS system, note how the changes to system records should be documented, and define a process for reviewing modified employee records for authorized changes.*

   SMD will create EPASS incident-handling procedures to record, resolve, and notify management of errors such as the one examined in this Report. The new procedures will include processes, documentation, and guidance for correcting and reviewing employee EPASS records. We will adopt portions of EPA's PII Incident Handling & Response Procedures, as applicable. Implementation milestone: Procedures will be in place by December 15, 2008.

3. *Create and implement procedures for the proper handling and disposing of defective ID badges.*

   SMD will create and implement procedures for handling and disposing of defective EPASS badges, consistent with National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization. Implementation milestone: Procedures will be in place by December 15, 2008.

We believe our corrective action plan and milestones meet OIG's requirements. If you have additional questions, please contact Personnel Security Branch Chief Kelly Glazier at 202-564-0351.

Attachment

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Administration and Resources Management
Director, Office of Administration, Office of Administration and Resources Management
Director, Security Management Division, Office of Administration and Resources Management
Agency Follow-up Official (the CFO)
Agency Follow-up Coordinator
Office of General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Audit Follow-up Coordinator, Office of Administration and Resources Management
Deputy Inspector General