U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Improvements Needed in EPA's Smartcard Program to Ensure Consistent Physical Access Procedures and Cost Reasonableness

Report No. 13-P-0200 **March 27, 2013**

Scan this mobile code to learn more about the EPA OIG.

Report Contributors:

Patrick Gilbride
Randy Holthaus
Raul Adrian
Lawrence Gunn
Kevin Lawrence

Abbreviations

CID	Criminal Investigation Division
DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
EPASS	Environmental Protection Agency Personnel Access and Security System
FAR	Federal Acquisition Regulation
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
GAO	U.S. Government Accountability Office
GSA	U.S. General Services Administration
HSPD-12	Homeland Security Presidential Directive-12
IGCE	Independent Government Cost Estimate
OAM	Office of Acquisition Management
OARM	Office of Administration and Resources Management
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
PACS	Physical Access Control System
PIN	Personal Identification Number
PIV	Personal Identity Verification
SMD	Security Management Division
SOP	Standard Operating Procedures

Cover photos: From left: a smartcard reader in the EPA Region 6 office in Dallas, Texas; EPA West, which is part of EPA headquarters. (EPA OIG photos)

U.S. Environmental Protection Agency
Office of Inspector General

13-P-0200
March 27, 2013

At a Glance

Why We Did This Review

Homeland Security Presidential Directive-12 (HSPD-12) and subsequent requirements state that inconsistent approaches to physical access are inefficient and costly, and increase risk to the federal government. We conducted this audit to determine whether the U.S. Environmental Protection Agency (EPA) upgraded physical access control systems consistent with the goals of HSPD-12 and subsequent requirements. We also evaluated whether EPA acquired and deployed smartcard technology in an efficient and effective manner.

This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthening EPA's workforce and capabilities.*

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

The full report is at:
www.epa.gov/oig/reports/2013/20130327-13-P-0200.pdf

Improvements Needed in EPA's Smartcard Program to Ensure Consistent Physical Access Procedures and Cost Reasonableness

What We Found

Contrary to its plans, EPA upgraded some less critical facilities prior to its most important facilities (including EPA headquarters). EPA stated it was more efficient to upgrade facilities based on geographic location rather than importance, but provided no quantitative data to support that position. In addition, EPA indicated it did not want to make mistakes upgrading headquarters buildings so it upgraded others first. As a result, some lower valued facilities required a higher level of authentication for access than EPA headquarters facilities.

The processes used to gain access are inconsistent and not yet inter-operable (can be used by all federal employees including those outside EPA) or intra-operable (can be used by any EPA employee). This occurred because EPA had not developed national physical access procedures to foster consistency. As a result, EPA is not realizing potential benefits associated with a standardized process.

EPA did not document assurance of cost reasonableness for some of the physical access control system contracts. EPA had spent over $12.8 million upgrading physical access control systems and could not assure that $3.8 million of that amount (30 percent) was spent in the most efficient and effective manner. EPA planned to award an additional $10.6 million to upgrade its systems.

Recommendations and Planned Agency Corrective Actions

We recommend that EPA re-prioritize the remaining facility upgrades by security level, from highest to lowest, and develop national policies and procedures that foster consistent inter-operable physical access. We also recommend that EPA establish an entity for overseeing EPA's smartcard program, conduct cost analysis of smartcard upgrades, and enforce guidelines for independent government cost estimates. EPA agreed with two of our five recommendations. For the other three recommendations, EPA proposed alternative corrective actions that we believe address our findings.

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

THE INSPECTOR GENERAL

March 27, 2013

MEMORANDUM

SUBJECT: Improvements Needed in EPA's Smartcard Program to Ensure Consistent Physical Access Procedures and Cost Reasonableness
Report No. 13-P-0200

FROM: Arthur A. Elkins Jr.

TO: Bob Perciasepe
Deputy Administrator

Craig E. Hooks
Assistant Administrator
Office of Administration and Resources Management

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determination on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

Action Required

The Agency did not concur with recommendations 1 and 2 and proposed acceptable alternative corrective actions. The Agency concurred with recommendations 3 and 4 and partially concurred with recommendation 5. On recommendation 5, parts c and d, the Agency provided acceptable proposed alternative corrective actions. We accept EPA's response and planned corrective actions for all five recommendations and no further response is needed. We have no objections to the further release of this report to the public. We will post this report to our website at http://www.epa.gov/oig.

We request that EPA provide the OIG with: (1) copies of the upgraded physical access control system planning documents submitted to the Office of Management and Budget in 2012; (2) its updated EPA Personnel Access and Security System project management plan; (3) the update to EPA Order 3200, *EPA Personal Identity Verification and Smartcard Program* when finalized; (4) a copy of its policy titled *Use of the PIV Card for Facility Access* when finalized;

(5) documents that demonstrate EPA's final decision on which office will oversee its smartcard program; and (6) a copy of any new guidance or policy issued that further details how and when independent government cost estimates should be prepared.

If you or your staff have any questions regarding this report, please contact Melissa Heist, Assistant Inspector General for Audit, at (202) 566-0899 or Heist.Melissa@epa.gov; or Patrick Gilbride, Product Line Director, at (303) 312-6969 or Gilbride.Patrick@epa.gov.

Table of Contents

Chapters

- continued-

Appendices

Chapter 1
Introduction

Purpose

On August 27, 2004, President George W. Bush signed Homeland Security Presidential Directive-12 (HSPD-12). The directive states, "it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." Agencies are still working to implement HSPD-12 and project milestones set by the Office of Management and Budget (OMB).

The purpose of this audit was to determine whether the U.S. Environmental Protection Agency (EPA) upgraded physical access control systems (PACS) consistent with the goals of HSPD-12 and subsequent requirements. We also sought to determine whether EPA acquired and deployed smartcard technology in an efficient and effective manner.

Background

In March 2007, in response to HSPD-12, EPA began issuing smartcards—the required common form of federal identification—to eligible EPA employees. EPA's physical resources include its office buildings, laboratories, storage centers, and other physical structures. PACS are the systems that control access to EPA's physical resources.

As of September 2011, EPA informed us it had 156 facilities nationwide. EPA planned to upgrade 65 of those 156 facilities with PACS. By the end of 2011, EPA had either completed or started upgrading 39 facilities. EPA plans to upgrade an additional 26 facilities by the end of 2014, and be HSPD-12 compliant by September 30, 2015.

EPA plans to spend a total of $55.8 million through fiscal year 2015 for its Environmental Protection Agency Personnel Access and Security System (EPASS) program. The EPASS program includes all components of personnel access, from developing and issuing ID cards (smartcards) to the technology and processes used to grant access to buildings and computers. According to data EPA provided OMB, EPA spent $32.2 million to upgrade smartcard technology through July 2011 (which includes upgrading computers as well as physical locations) and plans to spend about $23.6 million over the next 4 years for its EPASS program.

EPA is in the process of upgrading its PACS. In addition to providing access that is intra-operable throughout the Agency, EPA is required to upgrade PACS in a way that allows inter-operability with other federal agencies. For purposes of this report, intra-operability means that EPA employees can easily gain access to EPA facilities using their smartcards and PACS technology when they have an authorized business reason to do so.

EPA's Security Management Division (SMD) is responsible for upgrading PACS to comply with HSPD-12. SMD is within the Office of Administration and Resources Management's (OARM) Office of Administration (OA), which is responsible for the acquisition of all Agency facilities, property management, and property security. EPA's Office of Acquisition Management (OAM) is responsible for awarding and managing contracts, including those to implement HSPD-12. EPA's Office of Environmental Information (OEI) is responsible for upgrades related to computer and information systems needed to comply with HSPD-12.

Since the time President Bush signed HSPD-12 in 2004, the U.S. Department of Commerce and OMB developed documents that detail requirements and offer guidance for implementing the smartcard program:

- The U.S. Department of Commerce issued the Federal Information Processing Standards (FIPS) 201 in February 2005. FIPS 201 lays out the requirements for a common identification standard (to implement HSPD-12) for all federal employees and contractors. In March 2006, the U.S. Department of Commerce updated FIPS 201 by issuing FIPS 201-1.
- OMB issued M-05-24 in August 2005 to all federal departments and agencies to transmit HSPD-12 and provide associated guidance.
- OMB issued M-06-18 in June 2006 and established a set of parameters for acquiring products and services for implementing HSPD-12.
- OMB issued M-11-11 in February 2011, which included a memorandum from the U.S. Department of Homeland Security (DHS). The memo outlined a plan of action for agencies to expedite the full use of the smartcard credentials for access to federal facilities and information systems.

Scope and Methodology

We conducted our audit from June 2011 to November 2012 in accordance with generally accepted government auditing standards. Those standards require that we obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

During our audit, we reviewed HSPD-12 and other supporting federal criteria as well as EPA's policies and plans for implementing its smartcard program. We also reviewed relevant documentation for each of the contracts EPA awarded to upgrade physical and logical access control systems. We interviewed EPA headquarters managers and staff from OARM's SMD and OAM, and from OEI. We also conducted a site visit to Region 1 in Boston, Massachusetts, and interviewed PACS coordinators from all regions where EPA had upgraded PACS. Appendix A provides further details on our scope and methodology.

In addition to PACS, HSPD-12 involves upgrading logical access control systems. Logical resources include computers and information systems that EPA employees use. EPA has had limited accomplishments to date related to the Agency's logical access systems. EPA employees are not using smartcards to access information systems except for a limited number of employees who are testing their use. As a result, although logical access was originally within the scope of our review, we did not review logical access and developed no findings relating to that area.

Prior Audit Reports

Prior reports by the EPA Office of Inspector General (OIG), DHS OIG, GSA OIG, and U.S. Government Accountability Office (GAO) have highlighted various issues associated with implementing HSPD-12, including the complexity and the importance of sound planning across government. Appendix B provides details on the corrective actions EPA has taken to address prior audit report findings.

Chapter 2
EPA Did Not Upgrade Most Critical Facilities First

EPA upgraded some facilities that it classified as less critical prior to upgrading all of its most important and critical facilities, including headquarters facilities. On April 13, 2007, EPA issued Order 3200, *EPA Personal Identity Verification and Smartcard Program*. That order and subsequent plans stated that EPA would upgrade facilities in an order that would protect its most critical and valued assets first, but EPA did not do so. EPA officials said it was more efficient logistically to upgrade facilities based on geographic location rather than importance to EPA. However, SMD could not provide any analysis demonstrating efficiency. The SMD Director also said that EPA did not want to make mistakes upgrading its headquarters buildings so it has been upgrading other buildings first. As a result, some of EPA's most critical facilities do not require as stringent an identity verification process for access as some of its least important facilities. As of March 2012, EPA spent over $4.5 million to upgrade facilities it determined to be less critical to the Agency while it still has not upgraded all of its most critical facilities.

Implementation Plans Not Followed

Policy and plans indicate that EPA would upgrade its most critical assets before upgrading lower value assets (facilities). EPA designates the security level of its facilities numerically on a scale from 4 down to 1, based on a federal security standard. Level 4 facilities are EPA's most critical assets while Level 1 facilities would be least critical. According to the federal standard used for determining the security level of a facility, agencies should consider the following five factors when deciding the level assigned to a facility: (1) mission criticality, (2) symbolism, (3) facility population, (4) facility size, and (5) threat to tenant agencies.

EPA's Policy and Plans

EPA issued Order 3200 to establish the Agency's policy for providing a roadmap to implement EPA's smartcard program. The order states, "Systems located in facilities identified as Agency critical infrastructure assets will be replaced first, followed by Security Level 4 facilities, Security Level 3 facilities, and Security Level 2 facilities…Those EPA facilities designated at Security Level 1 will maintain existing physical access security counter measures."

EPA issued subsequent plans dealing with PACS upgrades. In 2008, EPA provided *OEI's HSPD-12 Physical Access Controls and Logical Access Controls Plan* to OMB. In 2009, EPA issued its EPASS Project Management Plan. Both plans laid out the priority in which EPA would upgrade PACS. They documented

that EPA would upgrade new construction or leases first, followed by facilities based on security level ratings. The 2008 plan stated, "…EPA will mitigate its highest risks first thus protecting our higher valued targets early on in the implementation process." The plan also stated that EPA would complete upgrading all of its Security Level 4 facilities by December 2011. Similar to EPA Order 3200, the 2008 plan also stated that existing Security Level 1 facilities would not be upgraded.

Inter-Agency Security Committee Standards

According to the *Interagency Security Committee (ISC) Standard: Facility Security Level Determinations for Federal Facilities*, Level 5 facilities are unique facilities with a high level of importance that merit the highest degree of protection. Level 4 facilities are also of high importance and require the next highest degree of protection, and so forth down to Level 1 facilities. EPA has classified all of the buildings housing EPA's 10 main regional offices as well as its headquarters facilities as Level 4.

EPA Upgraded 29 of Its Less Important Facilities Before Upgrading Its Most Critical Assets

EPA's SMD did not follow EPA Order 3200 or the last plan it submitted to OMB in 2008 for upgrading Agency facilities. Although EPA's stated policy was to upgrade its most critical assets first, as of the beginning of 2012 EPA had yet to start upgrades on six Level 4 facilities while it had completed or already started upgrades on 29 lower-level facilities. EPA also upgraded four Level 1 facilities and plans to upgrade another one even though its policies and plans stated that existing Level 1 facilities would not be upgraded. These lower-level facilities have less urgent security needs than the higher-level facilities. For example, one of the Level 1 facilities upgraded is used to store vehicles. No EPA employees work within that facility on a permanent basis. Conversely, EPA has not upgraded some of its headquarters buildings that are classified as Level 4, where up to hundreds and even thousands of EPA employees work on a full-time basis.

SMD plans to upgrade 65 facilities out of 156 EPA facilities by the end of September 2015. It plans to upgrade all Level 4 and Level 3 facilities, and some Level 2 and Level 1 facilities. By the end of 2011, EPA had completed or started upgrades to 39 facilities—4 at Level 1, 14 at Level 2, 11 at Level 3, and 10 at Level 4. EPA needs to complete upgrades for the following six Level 4 facilities

- Region 9 Main Building
- EPA East and EPA West in Headquarters
- Region 10 Main Building
- Region 7 Main Building
- Ariel Rios North and South Federal Building in Headquarters
- Ronald Reagan Building in Headquarters

Details on upgrade actions EPA has taken since 2006 and plans to take are in table 1.

Table 1: Number of EPA facilities to be upgraded by security level

Year started	Security levels				
	4	3	2	1	Total
2006	1	0	0	0	1
2007	2	2	2	0	6
2008	1	4	1	1	7
2009	0	0	1	0	1
2010	4	2	5	2	13
2011	2	3	5	1	11
2012*	3	1	2	0	6
2013*	3	5	4	0	12
2014*	0	0	7	1	8
Total to be upgraded	**16**	**17**	**27**	**5**	**65**
Total number of facilities	**16**	**17**	**82**	**38**	****156**

Source: OIG analysis of data provided by SMD.

* Projected by EPA.
** EPA has not assessed the security level for 3 of its 156 facilities.

Importance of Facilities Not a Priority for Initiating Upgrades

A facility's security level did not appear to be SMD's top consideration for when it should upgrade a facility. The SMD Director told us she believed it was more efficient and logistically made more sense to upgrade facilities based on geographic location. She said that SMD preferred to award one contract for each location or region and have all facilities in that area upgraded simultaneously. In other words, to install independent PACS across five facilities would require two servers (primary and backup) per location, totaling 10 servers across the five locations, and 5 vendor application licenses. In comparison, covering the five locations with a single enterprise implementation requires only two servers and one vendor application license. We requested that SMD provide data or documented justification showing that it was more efficient to upgrade based on location. According to the SMD Director, they did not have such data because the increased efficiency was obvious. However, without cost analysis, EPA cannot demonstrate that its approach was more efficient. Further, when we asked the Director why EPA's headquarters buildings were not upgraded first, the Director said that they did not want to make mistakes at headquarters and were therefore upgrading other buildings first and leaving the upgrades of headquarters buildings toward the end of the project. Although the Director said that efficiency was the primary reason EPA upgraded facilities in the order it did, criteria that EPA technical evaluation panel members used to review vendor proposals clearly stated that panel members should consider price/cost as the least important factor when evaluating which vendor should get a contract.

We also found two cases that further indicated that facility security levels were not the driving factor in the timing of upgrades. In one case, EPA upgraded the PACS system at a facility in Alabama that was 3 years overdue for a security level assessment. The facility was a Security Level 3 facility, so EPA should have re-assessed its Security Level every 3 years. According to SMD, EPA last assessed the facility in 2005. Therefore, EPA should have assessed the facility again in 2008 but it did not. EPA upgraded that facility while it had not upgraded many Level 4s. In another case, EPA upgraded a facility in Puerto Rico at the end of 2011 even though SMD did not complete the facility level assessment until January 2012.

We asked the SMD Director if she had considered other contracting approaches to upgrading facilities that emphasized security level first rather than all facilities in a given geographic area at the same time. She said that she had not thought of that and would have to consult with OAM to determine whether EPA could have used other contracting options. We discussed this issue with the OAM contracting officer for some PACS contracts and she told us that awarding contracts in order of facility security level could have been an effective alternative without resulting in greater cost. She said that SMD could have awarded national contracts at the beginning of this program to focus first on upgrading all Level 4s. She said that after SMD upgraded those facilities, additional national contracts could have been awarded to upgrade the Level 3s and so on, thereby addressing the most critical assets in a prioritized order.

Conclusions

Eight years after President Bush signed HSPD-12, EPA has not upgraded all of its most critical facilities. As a result, some facilities—housing hundreds or even thousands of employees along with other important assets—did not require the higher level of authentication to gain access as some of its facilities of lesser value and importance. As of March 2012, EPA had spent over $4.5 million to upgrade facilities assessed below Level 4 before it upgraded all Level 4 facilities. EPA has spent 69 percent more to upgrade Level 2 facilities ($2.8 million) as it has on Level 3 facilities ($1.66 million), even though Level 2 facilities are less critical than Level 3. As EPA stated in its formal plans, it planned to upgrade facilities with the highest security level classification before upgrading lower level facilities to improve security to its most critical assets first. However, EPA decided to deviate from the plan it submitted to OMB and instead upgraded facilities based on location. EPA should ensure it upgrades facilities based on the criticality of the facility rather than geographic location.

Recommendation

We recommend that the Assistant Administrator for Administration and Resources Management:

1. Re-prioritize the remaining facility upgrades by security level from highest to lowest, complete all remaining upgrades according to security level, and require the SMD Director to provide written justification for upgrading Level 1 facilities.

Agency Comments and OIG Evaluation

EPA did not concur with recommendation 1 and proposed an alternative recommendation. We continue to believe that EPA should have placed more effort into upgrading the Level 4 facilities earlier in this PACS upgrade project. The plan EPA shared in its response for upgrading its remaining facilities addresses this by planning to complete upgrades to facilities with higher security levels before completing those with a lower security level. Therefore, we agree with EPA's proposal to continue with its current sequencing of facility upgrades.

Regarding Level 1 facilities, we agree with EPA's proposal that the SMD Director will provide written justification to the Assistant Administrator for OARM and obtain approval in advance of any work. As a result, we consider recommendation 1 resolved with corrective action pending.

For EPA's detailed comments on this chapter and additional OIG responses, see appendix D.

Chapter 3
EPA's Physical Access Control Systems Not Inter-Operable or Intra-Operable

EPA has upgraded more than half of the 65 facilities' PACS it plans to upgrade, but the processes used to gain access vary considerably and the systems are not yet inter-operable or intra-operable in practice. For purposes of this report, intra-operability means that EPA employees can easily gain access to any EPA facility when they have an authorized business reason to do so, while inter-operability goes beyond EPA and applies to any federal employee that has a need for access. HSPD-12 and OMB's M-05-24 both stress the importance of eliminating inconsistency in physical access systems. EPA's varied and inconsistent approaches have resulted from a lack of developed, national physical access procedures to foster consistency or inter-operability. As a result, EPA is not realizing the potential benefits of a standardized process, and employee access to EPA buildings continues to be inconsistent depending on an employee's geographic location.

Physical Access Control Systems Should Be Inter-Operable

HSPD-12 stresses the importance of eliminating inconsistency in physical access systems, and states, "Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated." OMB M-05-24 states, "Inconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risk to the Federal government." OMB issued OMB M-11-11 in February 2011 incorporating DHS requirements that outlined a plan for federal agencies to use for upgrading identity verification systems. The DHS memo highlights the importance of using a consistent process for access. It states, "Specific benefits of the standardized credentials required by HSPD-12 include secure access to federal facilities.… Additionally, standardization leads to reduced overall costs and better ability to leverage the Federal Government's buying power with industry." This memo also states that "Agency processes must accept and electronically verify PIV [personal identity verification] credentials [smartcards] issued by other federal agencies."

FIPS 201-1 laid out the requirements for a common identification process. It addresses factors such as the ability to rapidly authenticate smartcards and to be inter-operable from one federal facility to another. FIPS 201-1 defines inter-operability as follows: "For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card."

OARM issued *Standard Operating Procedures for EPA Personnel Access and Security System (EPASS) Badge Post-Issuance Management*, dated June 23, 2011. While the procedures specify that EPA will have one process nationwide for issuing smartcards, it does not foster consistency in EPA's physical access process. Specifically, the procedures state that each location is individually responsible for figuring out how to allow employees to use the smartcards to gain access to EPA facilities. The EPASS standard operating procedure states:

> The scope of this SOP is to provide EPA personnel serving as an Issuer [of the smartcards] the same process and procedures across the entire EPA. It does not apply to integration of the EPASS card into EPA Physical Access Control Systems (PACS) or procedures for issuance of an initial card. Each site should develop their own PACS SOP to fulfill that requirement.

EPA Uses Various Processes for Physical Access Control

EPA is not using PACS in a consistent manner. EPA has used different processes, including the use of key pads and temporary cards, to gain access to EPA facilities. In addition, EPA's Criminal Investigation Division (CID) initially stated that it was not going to upgrade its facilities because it did not agree with the direction of the smartcard program, and SMD allowed that decision when it should not have.

Inconsistent Use of Card Reader Key Pads

EPA's use of key pads for physical access is inconsistent. Of the locations where PACS upgrades are complete, some use a card reader and key pad for access while others that have key pads do not use them. Regional security staff generally had rationale for using card readers with or without pin pads, but the reasoning was not consistent from one region to the next. In Region 6, the main building in Dallas, Texas, is a privately owned building, and because anyone from the general public can access the building, EPA Region 6 employees must enter a 6-digit personal identification number (PIN) in addition to scanning their smartcard. Further, we found that top-level managers in Region 6 intentionally never activated the card reader that controlled access between the Regional Administrator's office and the region's external affairs and legal offices, so staff who frequently go back and forth between those offices would not have to use their smartcards.

EPA also installed card readers with key pads throughout the areas it occupies in the Region 1 main building in Boston that several other federal agencies also occupy. However, employees only scan their cards for access; no PIN is required. Region 1 security staff informed us the key pads were in place in case additional security was necessary but there are no present plans to activate the key pads.

The more levels that an agency requires for access, the greater level of security provided. There are three basic levels of authentication an agency could use for access purposes – an agency could require an employee to use: (1) something they have in their possession (like swiping a smartcard across a reader); (2) something they know (like entering a PIN into the card reader in addition to just using the smartcard); and (3) something they are (like a biometric, such as a fingerprint or retinal scan, which is a feature unique to each person). If a facility or region required only the badge to be swiped across a card reader, an unauthorized person could use a lost or stolen card for access until it is deactivated.

In some regions, like Region 6, EPA requires employees to use something they have (card) and something they know (PIN). In other regions, EPA employees only use something they have (card) and do not have PINs assigned to them. In EPA headquarters buildings, employees have only used something they have (either their local EPA proximity card or smartcard) to present to security guards for access to those buildings. However, PACS readers have yet to be installed in all headquarters buildings.

Inconsistencies in Access by EPA Employees from Other Regions

The process EPA uses to grant access to visiting EPA employees also varies from one region to the next. For example, Region 6 requires a temporary visitor card and 8-digit PIN from EPA visitors from other regions to gain access. Region 8, on the other hand, uses a more traditional visitor check-in process. In Region 8, a visiting EPA employee checks in at a reception area at the main entrance and regional staff issue the person a visitor pass. Additionally, the visitor must rely on an EPA employee who resides in the building for access.

A temporary Region 6 visitor card. (EPA OIG photo)

Because PACS should be intra-operable, we asked Region 6 if it could program a visiting OIG employee's actual smartcard to allow them access in the region. While the Region 6 PACS coordinator informed us she could program the card to allow for access, she also warned that it could cause problems in the PACS identity verification system. She explained that because locations operate differently, changing the employee's information to allow access to Region 6 could adversely affect access when the employee returned to their home region. The 8-digit PIN that Region 6 requires for visiting EPA employees is a primary reason it uses the temporary card. EPA employees visiting Region 6 may use a different number of digits in their home region. If Region 6 were to provide access through that employee's smartcard, it would hinder their ability to access their home office.

We also asked Region 8 if it could program a visiting OIG employee's smartcard for use within that region. The Region 8 PACS coordinator said they were not

informed that they are required to do so and therefore would not, as it could cause problems within the PACS electronic identity verification system.

CID Not Required to Use Smartcard Readers

EPA's SMD also did not require one EPA office, CID, to use smartcard readers and additionally allowed them to forgo the PACS upgrade. CID did not seem to understand that it could maintain its unique security needs when upgrading its PACS. We found that CID's office in Dallas should have had a smartcard reader on one of its doors that the public could access. Once we brought this to the attention of SMD and CID, and after talking to CID's National Acting Director, CID started planning upgrades for more of its offices. CID will pilot the installation of smartcard readers in its offices in Regions 6, 7, and 9. If the pilot is successful, CID plans to install readers in offices in Regions 1, 2, 4, 5, and 10. In Dallas, EPA had already upgraded the main Region 6 building (a Level 4 facility) with card readers in 2011. Because CID's office space in Dallas was not upgraded at the same time as the Region 6 main building, EPA planned to spend an additional $17,927 to install the necessary equipment to CID's space. The SMD PACS project manager told us the CID space in Dallas would be upgraded by the end of February 2012. The additional card readers, including CID's main door that is accessible to the general public, were installed and operational in September 2012.

EPA Does Not Have National Procedures for Physical Access

According to its own plans, EPA knew it would take until September 2015 to complete its smartcard program—nearly 10 years. However, EPA has not developed national physical access procedures to foster consistency or intra-operability. EPA has already upgraded or begun to upgrade almost 70 percent of the facilities it plans to upgrade (45 of 65 facilities). We also determined that there was a lack of direct coordination between SMD and some regions. We interviewed PACS coordinators associated with each of the EPA facilities that had completed PACS upgrades, and some informed us that SMD did not communicate or provide guidance.

The SMD Director told us that an EPA workgroup has discussed issues related to the smartcard program across the country. According to the Director, the workgroup is made up of representatives from various programs and locations and is designed to resolve issues and determine necessary Agency-wide standards. In September 2012, the Director said that EPA would have national procedures in place by December 31, 2012.

Another reason the PACS upgrade process has been inconsistent is that SMD did not follow the plan submitted to OMB for carrying out the smartcard program. According to the SMD Director, the last time SMD submitted a formal PACS upgrade plan to OMB was in 2008. As discussed in chapter 2, EPA did not follow

the process it laid out in that 2008 plan. If EPA's plans and approach have changed, it should formally notify OMB of those changes so OMB can hold EPA accountable.

EPA Needs to Designate a Single Office to Administer Its Smartcard Program

At present, EPA does not have a clearly identified office in charge of its smartcard program. Program accountability is dispersed among offices and management. The Federal Identity, Credential, Access Management (FICAM) Roadmap and Implementation Guidance—issued in December 2011 by the Federal Chief Information Officers Council—lays out guidance for federal agencies to, among other things, increase security and improve inter-operability with the use of smartcards. In February 2011, OMB issued memorandum M-11-11 requiring agencies to follow the FICAM guidance. In M-11-11, OMB, through an attached memorandum from DHS, asked each agency to "…designate an agency lead official…" for implementing HSPD-12. While OMB asked agencies to designate one person, EPA designated two people as lead officials. EPA identified OARM's Director of the Office of Administration as well as EPA's Senior Agency Information Security Officer (within OEI) as lead officials for HSPD-12 implementation. SMD and OEI managers told us that they believe that EPA was the only agency that provided more than one point of contact to OMB.

According to the FICAM guidance, each agency should have a formal governance structure that creates and assigns a specific group to (a) provide oversight and management; and (b) develop and enforce agency-specific policies, processes, and performance measures. Oversight of the program could come from an executive steering committee and, if so (per the guidance), the committee should have a charter that establishes the group's authority to enforce changes to align the program with the agency's overall mission.

SMD and OEI managers told us that the Assistant Administrators for OARM and OEI have been discussing with EPA's Chief Financial Officer over the last year the idea of creating one office to oversee the Agency's smartcard program. In response to our draft audit report, EPA told us it plans to decide which entity will implement and oversee its smartcard program by June 30, 2013.

EPA Not Maximizing Efficiency and Security Within PACS

Because EPA has not established consistent national physical access procedures, regions have established different methods to gain access. With multiple processes to manage, EPA is not realizing the potential benefits of a standardized process such as lower equipment and maintenance costs and an overall greater understanding of how the process works. Furthermore, EPA cannot assure it is using the best approach nationally. If one physical access process is more effective than others, EPA should use that process nationwide. However, since

there is a lack of coordination among the different locations, good ideas used by one region may not be benefitting other regions.

Conclusions

We recognize that EPA operates under a culture where regions often establish their own processes for various programs. However, the inconsistency with which EPA has upgraded PACS is impeding EPA's ability to have intra-operable systems for EPA employees, much less inter-operability with other agencies. EPA should follow a national process for physical access to its facilities. Inter-operability is a primary goal associated with HSPD-12. Because the locations where EPA completed PACS upgrades are not intra-operable, EPA might have to spend additional funds to achieve national consistency. EPA has already spent over $12.8 million upgrading PACS. EPA should specify a consistent process for all regions to ensure that physical access systems can be inter-operable. EPA should also increase accountability over its smartcard program by clearly identifying one senior executive responsible for implementation and oversight. Stronger leadership over the program should help address the issues related to inconsistency that we have identified.

Recommendations

We recommend that the Assistant Administrator for Administration and Resources Management:

2. Develop national policies and procedures for PACS that foster consistent physical access to EPA offices around the country.

We recommend that the Deputy Administrator:

3. Establish one entity responsible for implementing and overseeing the Agency's smartcard program, including physical and logical access.

Agency Comments and OIG Evaluation

EPA did not concur with recommendation 2 in our draft report. EPA stated it disagreed with the word "inter-operable" in the recommendation because the EPASS badge is inherently intra-operable across the Agency and inter-operable with other federal agencies. EPA emphasized that the smartcard and PACS programs fully support inter- and intra-operability in compliance with all requirements and standards. As a result, EPA requested that the OIG remove the words "and inter-operable" from recommendation 2.

EPA stated that it agreed with the OIG that fostering consistent facility access procedures is important, with the understanding that procedures should be responsive to local security conditions and the range of real estate arrangements at

EPA facilities. EPA stated that what has been lacking is a clear understanding by all offices of the capabilities of the smartcards and PACS, as well as an Agency-wide policy on using smartcards for facility access. Therefore, EPA proposed in its response to do the following two things by no later than March 31, 2013: (1) disseminate information to regional personnel on existing capabilities of the smartcards and PACS, and (2) submit an EPA-wide policy titled *Use of the PIV Card for Facility Access* through the Agency's directives clearance process. The purpose of the policy is to provide consistent application of physical access controls; describe requirements for granting access to PIV-enabled EPA-controlled buildings and spaces; and define the roles and responsibilities of all parties involved in granting access to EPA facilities.

We removed the word "inter-operable" from the recommendation 2 language. We believe that EPA's planned efforts to educate regional personnel on the capabilities of the smartcards as well as to develop an Agency-wide policy to foster consistent access procedures are adequate corrective actions. We fully understand EPA's position that the EPASS badges are designed to be intra- and inter-operable, as the smartcards comply with FIPS 201 requirements. The issue that we presented in this chapter does not focus on any identified deficiencies with the smartcard (badge) itself but rather on how EPA has allowed the smartcards to be used for access in different ways across the country. EPA's planned corrective actions, particularly to issue a national policy on access procedures, should resolve the issues we identified during our audit. As a result, we consider recommendation 2 resolved with corrective action pending.

EPA concurred with recommendation 3. Under the Deputy Administrator's direction, EPA plans to determine the entity responsible for implementing and overseeing EPA's smartcard program by no later than June 30, 2013. We are pleased that discussions occurred over the last year between the Assistant Administrators for OARM and OEI and the Chief Financial Officer to consider creating one office to oversee the Agency's smartcard program. We consider recommendation 3 resolved with corrective action pending.

For EPA's detailed comments on this chapter and additional OIG responses, see appendix D.

Chapter 4
EPA Acquired and Deployed Smartcard Technology Without Assuring Costs Were Reasonable

EPA has not maintained sufficient documentation to make sound cost-related decisions for upgrading PACS. We found numerous independent government cost estimates (IGCEs) that were not prepared appropriately. For example:

- There was no evidence that some IGCEs were final.
- A cost estimator who was not employed at EPA was the only name on several IGCEs.
- At least one IGCE was prepared to match the winning contractor's proposed offer.
- For three PACS contracts, no IGCEs were prepared.

In addition, contracting officers did not certify that EPA bought only approved products and services that complied with HSPD-12 requirements. SMD did not have a process in place to analyze actual costs from completed upgrades for future cost estimating purposes due to issues within the program and contract management offices. SMD staff said they were not familiar with EPA OAM's IGCE Manual and GAO's cost estimating guide. OAM's contracting officers did not always ensure files contained necessary documentation of price reasonableness. EPA plans to spend an additional $10.6 million to upgrade PACS, and a lack of assurance that costs are fair and reasonable will remain if EPA continues to award contracts without conducting sound cost analysis.

Cost Data and Documentation Requirements

OAM is responsible for the policies, procedures, operations and support of EPA's procurement and contracts management program, from contract planning through closeout. In June 2010, OAM issued its most recent update to its *EPA Guide for Preparing Independent Government Cost Estimates*. This guidance states that IGCEs are an integral tool for effective acquisition programs in both government and private industry.

OAM's Manual for Preparing IGCEs

GAO's *Cost Estimating and Assessment Guide* (GAO-09-3SP) as well as OAM's IGCE Manual (June 2010 Revision) state that:

> … programs should be monitored continuously for cost control by comparing planned and actual performance against the approved program baseline [IGCE]… cost or schedule variances resulting

from incorrect assumptions should always be thoroughly documented so as not to repeat history, and all historical data should be archived in a database for use in supporting future estimates.

OAM's manual states an IGCE is a detailed estimate of the cost to the government to acquire services and/or supplies, typically from contractors. It also defines estimates as a projection or forecast of the economic or financial value of goods or services to be delivered in the future. IGCE users should be able to trace the data, calculations, modeling assumptions, and rationale back to the source document for verification and validation. In addition, it recommends that IGCEs contain the name and signature of the document preparer. A successful acquisition process requires collaboration between the program and procurement offices. When a program office prepares a meaningful IGCE, the contracting officer can use that document to facilitate the determination of fair and reasonable pricing in the procurement process.

OAM Contracts Management Manual

OAM's *Contracts Management Manual* states that project officers shall submit IGCEs for all contract actions, with a potential value in excess of $150,000 (the Federal Acquisition Regulation [FAR] threshold) for simplified acquisitions. In addition, it states, that IGCEs "are an integral part of any effective acquisition program." Section 7.3 of the manual specifies that the contracting officer will perform the necessary analysis leading to a decision to lease or purchase equipment considering comparative costs and other factors. It also states that the project officer and contracting officer share responsibility for making sure the procurement initiation package is complete. This package is required for all procurements above the FAR threshold.

FAR Requirements for Contract Documentation

FAR Part 4.801(b) states that the documentation in files shall be sufficient to constitute a complete history of the transaction. FAR Part 4.803(a) provides examples of records normally contained, if applicable, in contract files. These documents should include, but are not limited to, justifications and approvals, determinations, findings and associated documents, government estimate of contract price; a copy of each offer or quotation; source selection documentation; and cost or price analysis. FAR Part 4.803 also requires that federal agencies maintain documentation to evidence the contracting officer's determination of a fair and reasonable price. FAR 4.1302 states that agencies must purchase only approved personal identity verification products and services. When acquiring personal identity verification products and services not using GSA Federal Supply Schedule 70, agencies must ensure and certify that the applicable products and services are approved as compliant with FIPS 201.

EPA Did Not Maintain Sufficient Documentation to Support PACS Decisions

We obtained IGCEs for most of the projects, although there were no IGCEs for three. We also identified questionable IGCE preparation practices for PACS upgrades. Contract files for some PACS upgrades were incomplete. SMD was unable to provide us with evidence of detailed cost analysis for PACS projects.

Missing IGCEs

SMD was unable to locate IGCEs for the following three PACS upgrade projects: Potomac Yard, Arlington, Virginia; Fort Meade, Maryland; and Montgomery, Alabama. All of these projects exceeded the $150,000 FAR threshold, making it mandatory that an IGCE be prepared, per OAM's *Contracts Management Manual*. SMD paid contractors approximately $1.5 million for these three upgrades but was unable to produce IGCEs documenting SMD's assessment of what the cost should have been in each case. Specifically:

- *Potomac Yard project in 2006 (Contract GS07F0142L / EP06H001120):* EPA was unable to locate much of the documentation associated with this contract, other than a copy of the order, dated February 16, 2006, and a copy of Amendment 1 also from February 2006 that was a $4,623 de-obligation action to close out the file. Months after our original request, OAM was able to produce a copy of the Request for Quotes and correspondence related to bid evaluation. There was no IGCE for this project.

- *Fort Meade project started in 2008 (Contract GS-07F-7823C / EP-08H-000750 / EP-08H-001533 / EP-G11H-00126):* The file contained no documentation of contractor performance or IGCE.

- *Montgomery, Alabama, project in 2008 (Contract GS-Q7F-7823C / EP-10H-001546):* We found no IGCE in the file. SMD informed us it was unable to locate a copy of the IGCE for that contract.

Questionable IGCE Preparation Practices

We found that the contract file for the Region 1 main building upgrade in Boston contained an IGCE prepared by SMD's IGCE contractor consultant for the exact amount of the original procurement order for the primary PACS upgrade, or $2,322,852.08. When we asked the consultant about this, he acknowledged that he did not have support for the figures included in the IGCE and that he simply followed instructions from a former SMD manager to prepare an IGCE for the Boston project. The consultant told us that he "plugged" some numbers into certain cost categories on the IGCE template to make the total equal the contract award amount. He told us that he would not have done this on his own; someone

at EPA instructed him to do it that way. In that instance, the IGCE that EPA prepared was essentially meaningless as it was simply prepared to match the award amount.

We found several IGCEs that were not signed or dated and did not show evidence of EPA approval. Of 15 contracts we reviewed, 3 contained an IGCE prepared by the consultant. Through the end of 2011, documentation that we were provided showed that the consultant's estimates were considered by SMD to be the final IGCE. We found that those IGCEs prepared by SMD's consultant had the consultant's name at the top but neither SMD nor OAM personnel signed the estimates. The later IGCEs that the SMD contracting officer's representative prepared were not dated or signed by SMD or OAM staff. According to the contracting officer's representative, he now includes his estimates in the procurement initiation notice package. However, he did not sign them or have other evidence demonstrating that the IGCE was considered final and approved. SMD staff acknowledged that the consultant's estimate should not constitute the final estimate.

Contract Files for PACS Projects Incomplete

Contracts awarded between 2006 and 2010 were very poorly documented. In general, files did not contain evidence of contractor oversight, such as invoices, work progress reports, or certification of work completion. While both OEI and SMD acquired products and services from contractors that were not on GSA's Qualified HSPD-12 Service Providers list, OAM did not always certify that all products procured were approved and complied with all federal requirements. OAM managers and staff said Statements of Work that they develop require vendors to propose only approved products. In one case, SMD had scramble pad readers installed at Region 6's Addison, Texas, Continuity of Operations facility in 2009. According to SMD personnel, those card readers were not on GSA's approved products list in 2009 and EPA should not have installed them. The PACS readers installed at that facility cost more than $497,000, and do not comply with Section 508 of the Americans with Disabilities Act. Region 6 asserts that it never wanted them but SMD gave them no choice. Region 6 facilities personnel told us that they are requesting that SMD replace them to match the card readers in Region 6's main building.

SMD Did Not Analyze PACS Costs

SMD did not have a process in place to analyze actual costs from completed upgrades for future cost estimating purposes. In one case (Boston), SMD could not provide the actual cost of the PACS component of the installation contract. That contract included other security items such as closed circuit television. SMD said that the contractor quotes did not separate the price of the different components. As a result, this cost information was not available as a basis for comparison to evaluate subsequent procurements, as required by the criteria

documents cited above. EPA awarded other contracts that also contained costs for security features in addition to PACS. In some cases, regional EPA contacts provided information to clarify PACS costs, but SMD was not able to provide us with the appropriate documentation. SMD's contracting officer representative had, on his own initiative, attempted a comparison of contract costs in 2011 but was unable to include the above-cited contracts in the comparison. The contracting officer's representative acknowledged he is not required to perform this kind of analysis as a part of his regular duties and his supervisor—the PACS Project Manager—was unaware that he had attempted the analysis.

Project and Contract Management Staff Did Not Assure Adequate Data Were Maintained

Lack of cost data and incomplete contract files resulted from issues within both the project management and contract management offices. When the PACS upgrades started, staff and management turnover was an issue. Some employees with responsibilities for the PACS contracts left, and neither SMD nor OAM could locate some of the file documentation. In addition, OAM's contracting officers did not always ensure that the files contained necessary documents for some PACS contracts. SMD staff was not aware of the OAM IGCE Manual or the GAO *Cost Estimating and Assessment Guide*. SMD officials acknowledged they had not received training in this area. Further, SMD did not have a process in place to conduct and document cost analysis after projects were completed (for example, analyzing cost per reader/door, etc.) to gain assurance that future project costs were reasonable based on experience.

In July 2012, GAO issued a report titled *Information Technology Cost Estimation: Agencies Need to Address Significant Weaknesses in Policies and Practices* (GAO-12-629). GAO reported that EPA information technology investments only partially met requirements for complying with cost-estimating best practices, and did not meet requirements for providing cost estimating training. EPA also did not have a process to collect and store cost-related data. GAO concluded that until weaknesses are addressed, it will be difficult for EPA to use cost estimates to make informed decisions, formulate realistic budgets, or meaningfully measure progress for information technology projects.

Conclusions

EPA needs accountability for procurement decisions relating to PACS. SMD and OAM made procurement decisions without the benefit of required cost information. Of the $12.8 million EPA spent on PACS projects, it did not have the necessary documentation to show that the costs were fair and reasonable for $3.8 million (30 percent). In addition, EPA needs to ensure that it properly documents the cost analysis information in the future to ensure costs are reasonable and fair. According to EPA estimates, EPA plans to spend another

$10.6 million on PACs upgrades. EPA should conduct cost analysis on these future upgrades to ensure fair and reasonable prices.

There was no evidence that collaboration between SMD and OAM occurred. Furthermore, since the IGCEs were missing from some contract files, it appears that OAM did not use them at all in some cases. In addition, during the course of our review, SMD continually made revisions to the IGCEs that it had previously given us or changed its analysis. As a result, we were not confident that the data SMD was providing in the IGCEs was finalized or accurate.

Recommendations

We recommend that the Assistant Administrator for Administration and Resources Management:

4. Hold contracting officers accountable for maintaining complete files for PACS contracts, including documenting fair and reasonable price determinations, progress and completion of contracted work, and certifying that products for PACS procurements meet requirements in FAR Part 4.1302.

5. Enforce applicable guidelines pertaining to IGCEs, including:

    a. Preparing IGCEs for all procurement actions in excess of the FAR threshold.

    b. Adopting an official IGCE format that shall include the name and signature of the preparer, the date prepared, and the signature of the approving official.

    c. Establishing a process that SMD can use to conduct and document cost analyses of prior upgrades to ensure that future project costs are reasonable.

    d. Establishing a requirement that SMD staff involved with preparing and reviewing IGCEs certify that they have read OAM's IGCE Manual and understand the guidance.

Agency Comments and OIG Evaluation

EPA concurred with recommendation 4, stating that audit findings in this chapter are consistent with similar findings that OAM reviews have found related to internal controls and oversight systems. EPA responded that to ensure file quality, OAM conducts multiple types of contract file reviews. In these reviews, contract file content is a significant review element. Findings from these reviews are

provided to contracting officers for corrective action, if necessary, and used by OAM to identify policy gaps and possible training topics for contracting staff.

EPA stated in its response to recommendation 4 that it already completed corrective actions before the end of December 2012 that address our recommendation. We requested that OAM send us information related to any such actions. According to OAM, it has implemented a Balanced Scorecard Performance Management and Measurement Program, which contains a self-assessment and peer review and oversight component. A primary purpose of the Peer Review and Self Assessment Checklist, dated August 2012, is to conduct file reviews to assess the quality of the contracting process at EPA, including thorough file reviews. We reviewed this document and believe that, if followed, these reviews would address our recommendation, so we consider recommendation 4 closed upon issuance of this report.

EPA partially concurred with recommendation 5. Specifically, it agreed with recommendations 5a and 5b. For 5a, OAM stated that it agrees with the OIG that the IGCE policy as currently written does not distinguish between types of IGCEs or the level of detail required in IGCEs for different types of acquisitions. OAM agreed to review its current policy and provide more details and specific guidance pertaining to when an IGCE is required, at what threshold, and the level of detail required, to ensure the clarity, consistency, and significance of IGCEs prepared. OAM stated it would revise its policy by September 30, 2013. We agree with EPA's proposed action and consider this recommendation resolved with corrective action pending.

Regarding 5b, EPA responded that because each program in EPA is unique there is no "one-size-fits-all" IGCE format nor should there be. OAM agreed with the OIG that IGCEs should be thoughtfully prepared and reviewed. OAM is in the process of implementing EPA's Paperless Acquisition Program. This is an initiative that allows cost estimates to be included with electronically submitted procurement packages. This includes information on who developed and approved the procurement information. EPA plans to have the system implemented by September 30, 2013. We agree that this new system will address recommendation 5b and consider the recommendation resolved with corrective action pending.

Regarding recommendation 5c, OAM stated that the responsibility for conducting cost analysis resides with contracting officers, according to the FAR, and not with program offices. OAM further stated that its oversight program covers ensuring that cost analysis is performed. Regarding recommendation 5d, OAM said that training on IGCEs is part of the training that contracting officer representatives get before they are certified. As a result, OAM stated that it did not believe that a separate IGCE certification for SMD staff was necessary.

Regarding recommendations 5c and 5d, we accept OAM's rationale that cost analysis is to be performed by contracting officers. We also concur that OAM's IGCE training for new contracting officer representatives should address our recommendation. Therefore, we consider recommendations 5c and 5d closed upon issuance of this report.

For EPA's detailed comments on this chapter and additional OIG responses, see appendix D.

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	8	Re-prioritize the remaining facility upgrades by security level from highest to lowest, complete all remaining upgrades according to security level, and require the SMD Director to provide written justification for upgrading Level 1 facilities.	O	Assistant Administrator for Administration and Resources Management	06/30/2014		
2	14	Develop national policies and procedures for PACS that foster consistent physical access to EPA offices around the country.	O	Assistant Administrator for Administration and Resources Management	03/31/2013		
3	14	Establish one entity responsible for implementing and overseeing the Agency's smartcard program, including physical and logical access.	O	Deputy Administrator	06/30/2013		
4	21	Hold contracting officers accountable for maintaining complete files for PACS contracts, including documenting fair and reasonable price determinations, progress and completion of contracted work, and certifying that products for PACS procurements meet requirements in FAR Part 4.1302.	C	Assistant Administrator for Administration and Resources Management	12/31/2012		
5	21	Enforce applicable guidelines pertaining to IGCEs, including:		Assistant Administrator for Administration and Resources Management			
		a. Preparing IGCEs for all procurement actions in excess of the FAR threshold.	O		09/30/2013		
		b. Adopting an official IGCE format that shall include the name and signature of the preparer, the date prepared, and the signature of the approving official.	O		09/30/2013		
		c. Establishing a process that SMD can use to conduct and document cost analyses of prior upgrades to ensure that future project costs are reasonable.	C		12/21/2012		
		d. Establishing a requirement that SMD staff involved with preparing and reviewing IGCEs certify that they have read OAM's IGCE Manual and understand the guidance.	C		12/21/2012		

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

Appendix A

Details on Scope and Methodology

During our audit, we reviewed:

- HSPD-12 and associated criteria including FIPS 201 and OMB Memos M-05-24, M-06-18, and M-11-11
- EPA plans and policies regarding smartcard implementation
- All contracts that were awarded to upgrade physical and logical access control systems to comply with HSPD-12
- IGCEs and other cost-related documents for PACS contracts

During our audit, we interviewed:

- SMD's Director and Deputy Director, as well as the PACS project manager and other staff
- OEI Senior Agency Information Security Officer and staff
- EPA PACS coordinators from all regions where PACS were upgraded
- The EPA contractor who prepared PACS cost estimates for SMD
- OAM contract management staff
- DHS' Identity Management Division Chief

We issued a survey to individuals who SMD and OEI designated as primary contacts for physical and logical access systems. We issued the survey to ensure we received widespread input relating to EPA's progress in implementing HSPD-12.

We conducted a site visit to EPA's Region 1 located in the McCormack Building in Boston, Massachusetts. We selected Region 1 for a site visit because, of all of the completed upgrades, its upgrades were the most costly.

We coordinated with OMB's Assistant General Counsel on specific parts of its HSPD-12-related memos.

Appendix B

Prior OIG and GAO Audit Reports

EPA OIG Reports

Report number / date	HSPD-12 issues identified	Recommendations/corrective actions
09-P-0233, September 2009	EPA did not properly account for all property for implementing the issuance of smartcards under HSPD-12. The OIG found that: (1) four pieces of property valued at $29,538 were missing and not recorded in fixed assets subsystem, (2) acquisition costs in fixed assets subsystem were incorrect for some equipment, and (3) EPA did not accurately record required nonfinancial information for several pieces of property.	EPA needed to use established procedures to resolve accountability for the missing property, and review accuracy of HSPD-12 property information. EPA also needed to modify the HSPD-12 contract to reflect contractor requirements and accountability for using government property in government facilities. EPA established a December 2009 milestone for resolving missing HSPD-12 property and updating the Fixed Assets Subsystem with accurate records. The Agency also modified the contract on July 22, 2009, to reflect contractor requirements and accountability for the HSPD-12 property.
08-P-0271, September 2008	EPA did not require the EPASS contractor to follow Agency procedures for developing smartcards. EPASS did not have a certified Project Manager authorized to oversee the contractor's work. EPA also paid for contractor labor overcharges worth over $75,000.	EPA needed to (a) develop and maintain an EPASS System Management Plan, (b) appoint an EPASS Project Manager, (c) outline and reinforce compliance with EPA invoice reviewing guidance, and (d) ensure EPA collects from the contractor the amount EPA overpaid for billing rate errors. EPA agreed to address the recommendations contained in (a), (b), and (c) by January 2009. EPA reported it had already addressed recommendation (d) at the time its corrective action plan was issued.
08-P-0267, September 2008	An employee's ID card had the ID documents and other identifying information of another EPA employee. EPA procedures did not require EPASS staff to visually inspect employees' ID documents. EPA also lacked procedures for handling and disposing of defective smartcard badges.	EPA needed to (a) update card issuance procedures (including visually inspecting ID documents and comparing them to applicant), (b) create incident-handling procedures when errors occur, and (c) create and implement procedures for disposal of defective ID badges. EPA agreed with all three recommendations and planned to complete all three by December 2008.

DHS OIG Reports

Report number / date	HSPD-12 issues identified	Effects/recommendations
DHS OIG-10-40, January 2010	Resources and security issues hinder DHS' implementation of HSPD-12. DHS does not have a plan to implement successfully a robust program to increase physical and logical access security within the department. The absence of an HSPD-12 program implementation plan, department-wide deployment strategy, and sufficient resources are hindering progress. Components currently have their own individual physical access control systems, which will need to be consolidated into DHS' Headquarters PACS sometime in the future.	More work remains to ensure that DHS consolidates its infrastructures to support HSPD-12 program. In addition, DHS needs an interface between the card issuance system, Identity Management System, and PACS. Necessary facility upgrades need to be completed at component locations to ensure personal identity verification cards are inter-operable with DHS' physical and logical access control systems.
DHS OIG-08-01, October 2007	DHS has made progress but more work remains in meeting HSPD-12 requirements. DHS has not: (1) effectively managed the implementation to ensure that the department can meet all mandated milestones, (2) provided its components with sufficient guidance for their sites implementation of HSPD-12, (3) complied with OMB implementation reporting instructions, (4) identified to what extent PIV cards will be used or required in order to access facilities or information systems, and (5) determined which facilities will require PIV cards in order to gain physical access.	DHS does not have a certified and accredited operational system to support the implementation of HSPD-12. Specifically, DHS has not acquired the capability to issue PIV cards to its headquarters employees and contractors, and bring its system to production readiness.

GSA OIG Report

Report number / date	HSPD-12 issues identified	Effects/recommendations
GSA OIG A040111/P/R/R05002, January 2005	GSA hindered implementation of the smartcard credentials by a lack of a vision for incorporating the smartcard credential as a component of agency-wide security. As a result, the credentialing program will have only a limited impact on the security over physical access to buildings and facilities due to a variety of factors, including inconsistent controls and a lack of supporting infrastructure. Further, other aspects of the smartcard initiative—such as integrated security practices, inter-operability, and procurement issues—will also be problematic for an effective implementation.	Although GSA has provided guidance and procurement vehicles for agencies to implement smartcards, until recently it had made only limited progress in implementing smartcards within the agency.

GAO Reports

Report number / date	HSPD-12 issues identified	Effects/recommendations
GAO-06-178, February 2006	The federal government faces significant challenges in implementing FIPS 201. It will be a challenge to test and acquire compliant commercial products—such as smartcards and card readers—within required periods, and reconcile divergent implementation specifications. Incomplete guidance regarding the applicability of FIPS 201 to facilities, people, and information systems is a potential for substantial cost increases.	Until agencies address implementation challenges, the federal government may not fully realize the benefits of FIPS 201. Specifically, agencies may not be able to meet implementation deadlines established by OMB, and more importantly, true inter-operability among federal government agencies' smartcard programs—one of the major goals of FIPS 201—may not be achieved.
GAO-05-84T, October 2004	While smartcard technology offers benefits, launching smartcard projects—whether large or small—has proved challenging to federal agencies and efforts to sustain successful adoption of the technology remains difficult.	The successful adoption of smartcards throughout the federal government has been a challenging task, and federal agencies' adoption of this technology continues to evolve.

Appendix C

List of Contracts Awarded as of March 2012 for PACS Upgrades

#	Contract # / Order	Location	Actual Cost
1	GS07F0142L / EP06H001120	HQ: Potomac Yard, Arlington, VA	$560,229
2	RWA N0043821 Amendment #4	Region 6: COOP - Addison, TX	829,584
3	RWA B0334475	Region 1: HQ - Boston, MA	3,081,709
	RWA A0550220		
	RWA A0786418		
4	GS07F0103M DO#5	Cincinnati, OH: AWBERC, Norwood, Center Hill, Test and Evaluation; Erlanger, KY	393,374
5	GS07F0317K / EP09H001359	Region 8: HQ Denver, CO; NEIC, NETI (Lakewood, CO); Golden, CO; Helena, MT	900,477
	GS07F0317K / EP09H001605		
6	GS07F0317K / EP10H000322	Research Triangle Park: Mega Labs A/B, C, D/E, High Bay; NCC, FEELC, Page Road; Durham / Chapel Hill, NC	1,139,396
	GS07F0317K / EP10H001635		
	EP10H001578		
7	GS07F0317K / EP10H002003	Region 6: HQ - Dallas, TX	823,094
8	GS07F7823C / EP08H000750	Fort Meade, MD	255,763
	EP10H001533		
	GS-07F-7823C/ EP-GIIH-0012 6		
9	GS07F7823C / EP08H001546	Montgomery, AL	687,821
10	GS07F0450K / EP10H002195	Region 5: HQ, Lab; COOP - Willowbrook, IL	778,790
11	GS07F0489V / EP10H002230	Region 3: HQ - Philadelphia, PA; Boothwyn, PA; Linwood, PA; Wheeling, WV	530,394
12	GS-07F-0317F/ EP-G11H-00204	Ann Arbor Laboratory, MI	940,644
13	GS-07F-0178W/ EPG11H000667	Guaynabo, Puerto Rico	587,669
14	EP11H000874	Region 2: HQ - New York, NY; Edison Lab, Edison, NJ	1,481,898
15	GS07F450K / EPG11H00248	Region 4: HQ - Atlanta, GA; ERD, SESD, Athens, GA	983,985
Total			**$13,974.828** [1]

Source: EPA's SMD

[1] The dollar amounts in the table above, in some cases, are higher than the amount EPA spent specifically for PACS. This is because several of those contracts included costs for other security upgrades such as CCTV.

Appendix D

Agency Response

December 21, 2012

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY11-1789, "Improvements Needed in EPA's Smartcard Program to Ensure Consistent Physical Access Procedures and Cost Reasonableness," dated November 8, 2012

FROM: Renee Page
Director, Office of Administration

John R. Bashista
Director, Office of Acquisitions Management

TO: Melissa Heist
Assistant Inspector General for Audit

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. Following is a summary of the agency's overall position, along with its position on each of the report recommendations. For those report recommendations with which the agency agrees, we have provided high-level intended corrective actions and estimated completion dates to the extent we can. For those report recommendations with which the agency does not agree, we have explained our position and proposed alternatives to recommendations. We have also addressed selected factual inaccuracies in the report.

AGENCY'S OVERALL POSITION

Of the three major components of the federal smart card program–the badge, physical access control and logical access control–the Office of Administration is responsible for the first two. Regarding the primary subject of this draft report, physical access control, EPA is compliant with all applicable federal requirements and technical standards. We disagree with Recommendations 1 and 2 and all related text indicating we are not compliant. We agree with Recommendation 3. The report as a whole presents an inaccurate picture of the EPASS physical access control program. The majority of conclusions concerning physical access are not supported by sufficient and relevant evidence and are not logical inferences about the program.

Regarding the contracts-related portions of the report, the Office of Acquisition Management agrees with Recommendation 4; the findings in the draft report are consistent with similar findings under the Office of Acquisition Management's previous quality assurance program, which indicated a need to improve EPA's acquisition-related internal controls and oversight systems. OAM partially agrees with Recommendation 5, and believes the documentation supporting the sub-recommendations inflates the level of significance of the findings.

AGENCY'S RESPONSE TO REPORT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
3	Establish one entity responsible for implementing and overseeing the agency's smartcard program, including physical and logical access.	Under direction of the Deputy Administrator, relevant stakeholders will convene to determine the entity responsible for implementing and overseeing the program.	Q3 FY 2013
4	Hold contracting officers accountable for maintaining complete files for PACS contracts, including documenting fair and reasonable price determinations, progress and completion of contracted work, and certifying that products for PACS procurements meet requirements in FAR Part 4.1302.	See discussion below	Completed Q1 FY 2013
5a-b	Enforce applicable guidelines pertaining to IGCE, including: a. Preparing IGCEs for all procurement actions in excess of the FAR threshold. b. Adopting an official IGCE format that shall include the name and signature of the preparer, the date prepared, and the signature of the approving official.	See discussion below	a. Q4 FY 2013 b. Completed Q1 FY 2013

Recommendation 4

OARM/OAM agrees with this recommendation. Acquisition Handbook Chapters 4 and 42, and Contract Management Manual Chapters 7 and 42, contain significant policy and guidance pertaining to contract file documentation, such as required supporting documentation, approvals, and checklists. Findings in the Draft Report are consistent with similar findings under OAM's previous Quality Assurance Program which indicated a need to improve EPA's acquisition-related internal controls and oversight systems. As such, in FY 2011 OAM implemented the Balanced Scorecard (BSC) Performance Measurement and Management Program. Under the

BSC Program, OAM uses a combination of objective performance measures, quality assurance plans, self-assessment reviews, peer reviews, and training, to review, ensure and facilitate compliance with procurement statutes, regulations, policies, procedures, and other guidance.

To ensure file quality, OAM conducts multiple types of contract file reviews including: routine peer reviews and random sampling file reviews in accordance with contracting office Quality Assurance Plans (QAPs), and Self-Assessment Reviews under the OAM-wide Contract Management Assessment Program (CMAP) review. In each of these reviews, contract file content in terms of compliance and quality are meaningful review elements. Findings resulting from these reviews are provided to the Contracting Officers of record for corrective action if necessary, and are used by the organization to identify policy gaps, and as possible training topics for contracting staff.

Recommendation 5

As a general comment on the OIG's review in this area, OAM believes the documentation supporting these recommendations inflates the level of significance of these findings. Of the 22 files cited in the report, 18 were for the acquisition of supplies or services that meet the definition of a commercial item so a detailed IGCE is not required, 16 were acquired on a firm-fixed-price basis so a detailed IGCE is not required, 15 were for GSA Schedule orders so a detailed IGCE was not required, and 6 were valued at less than the Simplified Acquisition Threshold so an IGCE was not required. However, OAM continues to make efforts to ensure proper IGCEs are developed with new procurement packages as required by CMM 7.3.5.7. In October 2012, OAM released Interim Policy Notice 12-03 – *Acquisition Planning*, which puts greater emphasis on the combined planning efforts (including the development of IGCEs) of the program and contracting offices for each new acquisition greater than the SAT.

Sub-recommendation a: Having raised these anomalies, OAM agrees IGCE policy as currently written fails to distinguish between different *types* of IGCEs or the level of detail required in an IGCE for different types of acquisitions. As indicated above, many of the contract files reviewed in this audit were for commercial item products acquired competitively on a firm-fixed-price (FFP) basis through contracts managed by the General Services Administration (i.e. GSA Schedule Contracts). Competitive orders for FFP commercial item products through GSA Schedule Contracts do not rely on a detailed estimate of cost elements found in an IGCE as the basis for fair and reasonable pricing. In these instances, the most appropriate *type* of IGCE would be for a "Price Estimate" which the Federal Acquisition Institute (FAI) describes as "a bottom line firm-fixed price". Accordingly, OAM will review current policy to provide more details and specific guidance on the circumstances under which an IGCE is required, including at what threshold, as well as the content and level of detail and documentation required, to ensure clarity and consistency of IGCE's, and also to ensure IGCE's serve as meaningful tools in the acquisition process.

Sub-recommendation b: The *EPA Guide for Preparing Independent Government Cost Estimates, June 2010* published on OAM's web-site contains information and guidance on the types, methodologies, and techniques for developing IGCE's, as well as samples and approaches. However, emphasis on the program specific nature of the IGCE is a common theme throughout

the guide, and as such there is no way to develop a "one-size-fits-all" IGCE format. OAM does agree that IGCE's should be thoughtfully prepared and reviewed. To that end, OAM is currently developing a Paperless Acquisition Program to receive procurement documentation exclusively in electronic format through the Agency's acquisition system, EAS. EAS allows program offices with new contract requirements to attach supporting documents (including IGCEs) into an electronic requisition and route through the program office for review and approval. OAM believes creation of this electronic record will both increase the efficiency of the procurement process, but also satisfy sub-recommendation b.

Disagreements

No.	Recommendation	Agency Explanation/ Response	Proposed Alternative
1	Reprioritize the remaining facility upgrades by security level from highest to lowest, complete all remaining upgrades according to security level, and require the SMD director to provide written justification for upgrading Level 1 facilities.	See discussion below	Continue with current implementation sequencing, which in large part achieves the aim of the recommendation: all remaining Facility Security Level (FSL) 4 upgrades will have been initiated by Q2 FY13; all FSL 3s by Q3 FY13; all 2s by Q3 FY14. The SMD Director will provide written justification to the OARM Assistant Administrator for any FSL 1 upgrades.
2	Develop national policies and procedures for PACS that foster consistent and inter-operable physical access to EPA offices around the country.	See discussion below	Submit for EPA directives clearance process a draft EPA-wide policy, *Use of the PIV Card for Facility Access*, Q2 FY 2013. Create and disseminate outreach on existing inter-operable capabilities to regional personnel, Q2 FY 2013.

No.	Recommendation	Agency Explanation/ Response	Proposed Alternative
5c-d	Enforce applicable guidelines pertaining to IGCE, including: c. Establishing a process that SMD staff can use to conduct and document cost analyses of prior upgrades to ensure that future project costs are reasonable. d. Establishing a requirement that SMD staff involved with preparing and reviewing IGCEs certify that they have read OAM's IGCE Manual and understand the guidance.	See discussion below	N/A

Recommendation 1

OA disagrees with Recommendation 1 for the following reasons (explained in more detail below): Facility security level is one, but not the only, criterion for prioritizing PACS projects; the rationale for the recommendation, "...some facilities housing hundreds or even thousands of employees along with other important assets did not require the higher level of authentication to gain access as some facilities of lesser value and importance" (p. 7) is not supported by evidence and confuses the role of authentication; and any reprioritizing at this advanced stage of the overall PACS project would be costly and unnecessary, particularly since the remaining sequencing in large part accomplishes the aim of the recommendation.

OIG Comment: At the time we completed our work, EPA had not upgraded Security Level 4 facilities within headquarters. Access to these facilities is gained by showing a badge to a security guard rather than using a smartcard badge and a PACS reader. Conversely, in other locations, EPA did update some lower level facilities with PACS readers. In one case, EPA upgraded a vehicle storage building that did not permanently house any EPA employees. EPA's most critical assets, where more people and other important resources reside, should be upgraded before its lower level facilities.

Security level is not the only criterion for prioritizing: EPA's PACS program is accountable to OMB, and nowhere does OMB stipulate that PACS be upgraded according to facility security level (FSL). The report's statement, "Eight years after President Bush signed HSPD-12, EPA has not upgraded all of its most critical facilities," (p. 7), is not relevant since OMB leaves sequencing to the agencies. EPA is fully compliant with its OMB plan, which is to install PIV-enabled PACS at 5-8 facilities per year, with completion by the end of FY 2015.

OIG Comment: In 2008, EPA provided *OEI's HSPD-12 Physical Access Controls and Logical Access Controls Plan* to OMB. In 2009, EPA issued its EPASS Project Management Plan. Both plans laid out the priority in which EPA would upgrade PACS. They documented that EPA would upgrade new construction or leases first, followed by facilities based on security level ratings. The 2008 plan stated, "…EPA will mitigate its highest risks first thus protecting our higher valued targets early on in the implementation process." The plan also stated that EPA would complete upgrading all of its Security Level 4 facilities by December 2011. Similar to EPA Order 3200, the 2008 plan also stated that existing Security Level 1 facilities would not be upgraded. We continue to believe that EPA did not follow the plan as submitted to OMB.

Likewise, HSPD-12 and its implementing standards do not stipulate PACS sequencing or that PACS be upgraded according to FSL. FSL is derived from an Interagency Security Committee (ISC) 2008 standard, *Facility Security Level Determinations for Federal Facilities*. That standard defines FSL as a "categorization based on the analysis of several security-related facility factors, which then serves as the basis for the implementation of certain protective security measures specified in other ISC standards" (p. 2), not in HSPD-12 standards. EPA complies with the ISC's 2010 *Physical Security Criteria for Federal Facilities* to mitigate vulnerabilities by FSL-appropriate means, agency wide, including vulnerabilities related to facility access controls. The ISC standard does not mention PIV-enabled PACS among physical access control protective measures.

OIG Comment: EPA's comments in the preceding paragraph do not include all of the criteria for which it was accountable. EPA did not follow the process for upgrading the PACS program that was defined in the plans it submitted to OMB in 2008 or EPA Order 3200—the Agency's policy for implementing EPA's smartcard program. Our report does not recommend any changes to processes and procedures where EPA is already compliant. Instead, our recommendations target those areas where EPA has not been compliant.

EPA's PACS sequencing has evolved since 2005, as is appropriate, to reflect new and changing technical standards, federal priorities, enhanced technology, the ability to network PACS, lessons learned, and opportunities to decrease waste and improve efficiency and cost effectiveness. EPA considers FSLs in sequencing PACS upgrades, but also considers existing PACS that are failing, new construction or leases, and facilities housing critical infrastructure and key resources. Please note that at EPA, some critical infrastructure and systems (such as those in COOP facilities) are housed in facilities that, per ISC standards, are FSL 1 or 2 because of their small size, small population and lack of symbolic importance.

On a case-by-case basis, certain facilities that are in close proximity to priority PACS implementation sites and that would eventually be scheduled for PACS upgrades are included with nearby, higher-priority projects to reduce cost, improve efficiency, and align IT infrastructure. To give a dramatic example of the cost efficiencies gained:

- At an earlier phase of the PACS program, the Region 6 Addison and Dallas facilities, with approximately 150 card readers between them, were upgraded under separate contracts for a combined cost of $1,283,665.

- The Region 2 New York and Edison facilities, with over 200 card readers between them, were upgraded under a single contract at a cost of $909,290.

OA agrees with the OIG that we should have updated documents that referenced the sequencing plans. We have revised the PACS-related section of our 2012 submission to OMB to reflect our current sequencing considerations (although that is not required) and we have updated our EPASS project management plan. EPA Order 3200, *EPA Personal Identity Verification and Smartcard Program*, will be updated in CY 2013 by a one-EPA team of stakeholders, and any reference to PACS sequencing will be deleted.

OIG Comment: We are pleased that EPA agrees that they should have updated these critical documents earlier. These official documents stated EPA's plans for upgrading facilities in terms of the number to be upgraded and by what date. The documents represented the official EPA plans and as such should have been revised when SMD knew it was changing its plans.

Authentication is not a sequencing issue: The following OIG conclusions reflect a misunderstanding of the role of identity verification and authentication:

- "...some of EPA's most critical facilities do not require as stringent an identity verification process for access as some of its least important facilities" (p. 4).
- "...some facilities housing hundreds or even thousands of employees along with other important assets did not require the higher level of authentication to gain access as some facilities of lesser value and importance" (p. 7).

First, no federal mandate or standard, including the HSPD-12 implementing standard FIPS 201-1, stipulates that identity verification or authentication determine the order of PIV-enabled PACS implementation. Per FIPS 201-1: "PIV Cards can be used for identity authentication in environments that are equipped with card readers as well as those that lack card readers" (p. 46). FIPS 201-1 defines authentication as: "The process of establishing confidence of authenticity; in this case in the validity of a person's identity and the PIV card" (p. 70). In addition, 99% of EPA federal employees (95% of all personnel when non-federal employees are included) have completed HSPD-12-mandated identity verification and authentication in the form of a background investigation, identity proofing, and PIV card/EPASS badge issuance.

OIG Comment: The comments in the preceding paragraph relate to requirements for smartcard identification badges. The content in our report deals with EPA's implementation and use of PACS along with the smartcard badge. The smartcard badges are just one piece of the overall physical access process. Our report raises issues EPA needs to address to improve its overall process for physical access.

Second, OIG conclusions are based on subjective characterizations of facilities as "most critical (p. 4)," "less critical (At a Glance), "least important (p. 4)," "most important (At a Glance)," "critical and most valued (p. 4)," "of lesser value and importance (p. 7)." No physical security standard or smartcard mandate ranks buildings as most or least

important, most or least critical, or most or least valuable. Although the report claims to cite the ISC *Facility Security Level Determinations for Federal Facilities*, "Level 4 facilities are also of high importance and require the next highest degree of protection, and so forth down to Level 1 facilities" (p. 5), the ISC standard does not state that. Per ISC standards, protective measures are based on a risk management system that considers FSL, identification of a baseline Level of Protection (LOP), and determination of acceptable levels of risk. Again, PIV-enabled PACS are not among the protective measures addressed in the ISC *Physical Security Criteria for Federal Facilities*.

OIG Comment: The document titled *Facility Security Level Determinations for Federal Facilities* explains and defines the hierarchy of rankings that federal agencies should use to determine the level of each facility. That document states that the higher the designated level of a facility the more valuable and critical that facility is to achieving an agency's mission. It also states that the degree of protection should be commensurate with each designated security level, with higher security levels requiring greater protection. While the standard titled *Physical Security Criteria for Federal Facilities* may not specifically discuss PIV-enabled PACS, the purpose of the smartcards and related systems are to increase and improve security and protection.

The OIG's conclusion that the agency's PACS upgrade sequencing has somehow left "hundreds and even thousands of EPA employees" (p. 5) at risk is not logical and not supported by fact. The agency mitigates risk and vulnerability at all facilities per ISC standards, in which PIV-enabled PACS figure not at all.

OIG Comment: As stated in our comment above, Security Level 4 facilities, by definition, are higher value assets, and EPA states the same in the plan it submitted to OMB in 2008. Further, having operational PACS in place at such facilities provides an additional layer of security by increasing the number of levels of authentication needed to gain access. EPA asserts that PACS systems do not add security over what was in place. If PACS systems add no additional security, this raises the question why EPA would plan to spend nearly $56 million on this program. EPA is complying with HSPD-12 and subsequent requirements because the smartcard and associated systems increase security and safety, which was the intent behind HSPD-12.

The majority of upgrades have already been initiated: Making changes to PACS sequencing at this late stage of the program would be costly, disruptive and unnecessary, not only for the reasons above, but because the remaining schedule largely accomplishes the aim of the OIG recommendation. The contracts for the remaining Level 4 upgrades will be awarded in Q2 FY 2013. All remaining Level 3 upgrades are scheduled for award by Q3 FY 2013 and all remaining Level 2 upgrades by Q3 FY14.

Proposed Alternative:
Continue with current implementation sequencing, which in large part achieves the aim of the recommendation: all remaining FSL 4 upgrades will be initiated by Q2 FY 2013; all FSL 3s by Q3 FY 2013; and all FSL 2s by Q3 FY14. The SMD Director will provide written justification to the Assistant Administrator of OARM for any FSL 1 projects.

OIG Comment: We agree with EPA's proposed alternative to complete Security Level 4 facilities before completing upgrades to lower level facilities, and that the SMD Director will provide written justification to the Assistant Administrator for OARM prior to updating any Security Level 1 facilities.

Recommendation 2

Our disagreement is with the presence of the word "inter-operable" in the recommendation and the misunderstanding it represents. The EPASS badge, per FIPS 201 requirements, is inherently intra-operable across the agency and inter-operable with other agencies. Within EPA, any EPASS badge can be authenticated and granted access to any PIV-enabled PACS. EPA PIV-enabled PACS can authenticate PIV cards issued by other agencies, and our EPASS badges are accepted at other agencies' PIV-enabled PACS. The EPASS badge and PACS programs fully support inter- and intra-operability in compliance with all governing authorities and technical standards; all statements in the draft audit indicating otherwise are incorrect (see additional comments on accuracy of draft report, below).

OIG Comment: We understand that the EPASS badge is designed and produced to have the capabilities to be both intra- and inter-operable and we do not question that in this report. The point we make in chapter 3 is that, in practice, these security systems at EPA facilities across the country are operated in dissimilar ways and were not fostering consistent access to facilities by EPA employees. We believe that EPA's response is one related to semantics rather than substance as EPA states that it has been lacking nationwide policies and procedures that foster consistent facility access using the smartcard (see next OIG comment).

What is lacking is not intra- and inter-operability, but rather: 1) a clear local understanding of the intra- and inter-operable capabilities of Personal Identity Verification (PIV) cards and existing PACS; and 2) agencywide policy on use of the PIV card for facility access. The proposed alternative below addresses both of these issues. We agree with the OIG that fostering consistent facility access procedures is important, with the understanding that procedures need to be responsive to local security conditions and the wide range of real estate arrangements at EPA. One size cannot fit all when circumstances include EPA-owned and leased, privately owned, GSA-owned and leased, single and multi-tenant, and mixed federal and private tenant arrangements.

OIG Comment: We agree with EPA that what has been lacking is a national EPA-wide policy and procedures for ensuring consistent access procedures for all EPA employees.

Proposed Alternative:
OARM requests that the words "and inter-operable" be removed from Recommendation 2 so that we can fully agree with the text. We are planning to foster consistent facility access control procedures and improve regional understanding of intra- and inter-operable capabilities of existing PACS. To achieve this, OARM will create and disseminate to regional personnel outreach on existing inter-operable capabilities in Q2 FY 2013. EPA will also submit for the directives clearance process an EPA-wide policy, *Use of the PIV Card for Facility Access*, in Q2 FY 2013. The policy is the result of a one-EPA effort and addresses the requirements for permitting unescorted access to EPA facilities where physical access is controlled by a PIV-enabled PACS. The purpose of the policy is to:

- Provide consistent application of physical access controls
- Describe requirements for granting access to PIV-enabled EPA-controlled buildings and spaces
- Define the security roles and responsibilities of all parties involved in granting access to EPA facilities

OIG Comment: We removed the words "and inter-operable" from recommendation 2 in our draft report. As currently implemented, EPA's PACS and smartcard badges do not allow consistent facility access to EPA and other federal employees as intended. We do agree with EPA's proposed recommendation to develop and implement a policy that will allow for consistent facility access control procedures and improve regional understanding of intra- and inter-operable capabilities before March 31, 2013.

Recommendation 5c-d (see general comment under Recommendation 5, above)

Sub-recommendation c: The intent and basis for this recommendation is unclear, and as such, OAM is unable to provide a response without further clarification/information from the OIG. The FAR (3.501-2, 15.305, 15.402, 15.404, 15.405, 15.406, 43.204) sets forth responsibility for conducting cost analysis with the Contracting Officer. Accordingly, the recommendation to establish a process to ensure SMD conducts cost analysis assigns responsibility for this critical function contrary to regulation. With regard to ensuring adequate cost analysis is performed, OAM's oversight program is described in the response to recommendation 4 above.

OIG Comment: The intent of this recommendation is to ensure that SMD considers cost through meaningful analysis before spending taxpayer dollars on its programs. We are not suggesting that OARM removes responsibility from contracting officers. We believe cost analysis is a useful and necessary process across all programs and divisions that use contractors to carry out EPA's mission. The *EPA Guide for Preparing Independent Government Cost Estimates*, prepared by OAM, states, "The FAR considers IGCE's an integral part of the acquisition process. A successful acquisition process requires collaboration between the program and procurement offices. When a Program Office prepares a meaningful IGCE, the CO may use that document to facilitate the determination of fair and reasonable pricing in the procurement process. As a result, all parties benefit from a well prepared IGCE."

Sub-recommendation d: OAM makes training on IGCE's available to through various OAM sponsored and conducted training sessions. Additionally, under the new three tiered COR training and certification program, OAM will continue to ensure the COR curriculum includes training on IGCE's. Accordingly, completion of IGCE training is incorporated under COR certification. As a result, OAM believes that the separate IGCE training certification recommended by the OIG is both redundant and unnecessary.

OIG Comment: We agree with the action EPA has taken to make IGCE training available. However, in a face-to-face interview on March 20, 2012, in Washington, DC, the SMD PACS project manager and an SMD contracting officer representative both told us that they: (1) were not familiar with the EPA Guide for Preparing Independent Government Cost Estimates or the GAO Cost Estimating and Assessment Guide, and (2) had not been offered any training on preparing IGCEs in general. Therefore, EPA should ensure that appropriate staff are aware of available IGCE training and take the training.

Some Additional Factual Inaccuracies in the Draft Report

OA requests that the following indirect quotations attributed to SMD Director [name removed] be removed from the report. The OIG versions of her words do not reflect what she said, create an unwarranted and unsubstantiated negative personal portrayal and do not qualify as relevant evidence (emphasis added):

- "The SMD Director also said that EPA did not want to make mistakes upgrading its headquarters buildings so it has been upgrading other buildings first" (p. 4). The report repeats this inaccurate claim in two other places: "Also, EPA indicated it did not want to make mistakes upgrading headquarters buildings so it upgraded others first" (At a Glance), and "The Director said that they did not want to make mistakes at headquarters and were therefore upgrading other buildings first and leaving the upgrades of headquarters buildings toward the end of the project" (p. 6).

OIG Comment: During a June 21, 2011 meeting with the SMD Director, we questioned the decision not to upgrade Headquarters' buildings before other lower level facilities. We believe the statements in the report accurately paraphrase those discussions.

- "The SMD Director told us she believed it was more efficient and logistically made more sense to upgrade facilities based on geographic location. She said that SMD preferred to award one contract for each location or region and have all facilities in that area upgraded simultaneously. SMD could not provide data or documented justification showing that it was more efficient to upgrade based on location; the Director said SMD did not have such data because the increased efficiency was obvious" (p. 6)**.**

OIG Comment: On December 14, 2011, the SMD Director sent the OIG an email that stated:

> "Implementing PACS facility-by-facility requires separate and distinct systems to be installed in each individual facility. Several criteria were considered when comparing a facility-based approach to an enterprise approach. These criteria included the cost of hardware and software and the increased technical complexity caused by the volume of systems. No quantitative data was produced because of the obvious cost advantage. For example, to install independent PACS across five facilities would require two servers (primary and backup) per location, totaling 10 servers across the five locations, and 5 vendor application licenses. In comparison, covering the five locations with a single enterprise implementation requires only two servers and one vendor application license. The cost differential is obvious without a detailed quantitative analysis."

- "We asked the SMD Director if she had considered other contracting approaches to upgrading facilities that emphasized security level first rather than all facilities in a given geographic area at the same time. She said that she had not thought of that and would have to consult with OAM to determine whether EPA could have used other contracting options" (p. 7)**.**

OIG Comment: We asked the SMD Director on December 21, 2011, whether SMD had considered the possibility of awarding a national contract to first upgrade Security Level 4 facilities that would contain the option to go back to a particular geographic area at a later time to upgrade lower-level facilities in that same location. The SMD Director said to us that she had never thought of that option and she would need to consult with a contracting expert in OAM to determine whether that was feasible.

We request deletion of unsupported speculation on what might have been effective contracting in 2006 or what might have been done at that time. The OIG presents conjecture on a complex issue by an individual who likely did not identify herself to the OIG as expert in the identification of EPA's "most critical assets" or in what constitutes a proper "prioritized order" for PACS sequencing. This text does not qualify as relevant evidence and does not contribute to logical inferences based on findings (emphasis added):

- "We discussed this issue with the OAM contracting officer for some PACS contracts and she told us that awarding contracts in order of facility security level could have been an effective alternative without resulting in greater cost. She said that SMD could have awarded national contracts at the beginning of this program to focus first on upgrading all

Level 4s. She said that after SMD upgraded those facilities, additional national contracts could have been awarded to upgrade the Level 3s and so on, thereby addressing the most critical assets in a prioritized order" (p. 7).

OIG Comment: We discussed possible contracting options with an EPA contracting officer responsible for awarding PACS contracts. The contracting officer provided us with her views on additional options mentioned in the report. We believe that this contracting officer would have the knowledge and background to provide credible contracting options for awarding PACS contracts.

We request deletion or correction of all statements indicating EPA has not achieved intra- and inter-operability; EPA has achieved full intra- and inter-operability (see discussion of Recommendation 2, above).

OIG Comment: EPA has achieved the potential for intra- and inter-operability through the EPASS badge. However, the use of the smartcards and the physical access control systems is not consistently applied across EPA. We agree with EPA that it needs nationwide policies and procedures that foster consistent facility access using the smartcard and we encourage the Agency to finalize those policies and procedures as soon as possible.

We request deletion of the following inaccurate statement: "Another reason the PACS upgrade has been inconsistent is that SMD has not been accountable for how it is carrying out the program" (p. 11). SMD is accountable to the agency and OMB and provides all reporting that the agency and OMB require. Our PACS accountability includes:

- A monthly data call to OMB on earned value management, performance and risk management, including PACS schedules and costs
- An updated EPASS implementation plan sent to OMB in July 2012
- An annual data call to OMB for EPA's PortfolioStat in June 2012
- A yearly Capital Planning and Investment Control (CPIC) report to OMB
- An annual report on EPASS, including PACS, as part of the Federal Managers Financial Integrity Act assurance process
- A yearly Chief Information Officer CPIC investment review

OIG Comment: We deleted the statement from our draft report that SMD has not been accountable for carrying out the program. We agree that SMD generates a number of reports for OMB. Our position is that EPA does not have a clearly identified office in charge of its smartcard program. Responsibility for the program is split between OARM and OEI.

The OIG makes incorrect connections between accountability, leadership and inconsistency (emphasis added). "EPA should also increase accountability over its smartcard program by clearly identifying one senior executive responsible for implementation and oversight. Stronger leadership over the program should help address the issues related to inconsistency that we have

identified" (p. 13). The inconsistency referenced here refers to an earlier OIG statement: "However, the inconsistency with which EPA has upgraded PACS is impeding EPA's ability to have intra-operable systems for EPA employees, much less inter-operability with other agencies" (p. 13). As explained in our response to Recommendation 2, the PACS program has achieved full intra- and inter-operability; as explained in the previous paragraph, our PACS program is already accountable to EPA and OMB. We agree that a single entity to oversee the smartcard program is needed to make the agency compliant with OMB Memorandum M-11-11 and position the program to implement EPA's Identity, Credential, and Access Management initiative.

OIG Comment: EPA implemented this program from 2008 through 2012 in a manner that was not consistent with the plan submitted to OMB. We recognize that SMD responded to this issue identified during our audit by submitting a revised plan to OMB in July 2012. This was a positive step to increasing accountability. However, EPA's accountability for implementing the PACS program is diminished without identifying a senior executive responsible for the PACS program. Regarding the second part of the paragraph above, EPA is not implementing the physical access control system in a consistent manner. Different locations use different procedures for access and there has been no national standard to guide this process.

The following OIG language is unnecessary and inflammatory (emphasis added): "In addition, EPA's Criminal Investigation Division (CID) initially stated that it was not going to upgrade its facilities because it did not agree with the direction of the smartcard program, and SMD allowed CID to dictate that decision when it should not have" (p. 9). CID did not interact with SMD in this manner. The two organizations have been collaborative and collegial. We request that the underlined text be removed.

OIG Comment: In discussions with CID and SMD, we found that CID Dallas, Texas, elected not to participate in the program. SMD did not take action to ensure CID was included in the program until we pointed out to them that the space was accessible to the general public. We have adjusted the report language to this effect.

The table on p. 6 of the report, as well as information derived from the table throughout the report, does not accurately reflect the data provided by SMD to the OIG. To give one example, the OIG counts only one FSL 4 facility at Research Triangle Park; however, SMD upgraded PACS at multiple FSL 4 facilities there.

OIG Comment: During this audit, EPA provided us with multiple lists of EPA facilities that were different and some contained discrepancies. Further, in some spreadsheets SMD provided us they counted a location as one facility and in others they counted each building at that location as a separate facility. Therefore, to obtain a list that incorporated total facilities by security level and the date of upgrades, we developed the best supportable list that we could from the data SMD provided. We based table 1 on data SMD provided as of April 2012. Because EPA's lists combined facilities into a single entry in some cases, we acknowledge that the actual number of EPA facilities could be higher than the total included in our table. Based on a report we received from SMD that EPA submitted to OMB, as of July 2012 EPA planned to upgrade a total of 76 facilities (21 level 4s; 26 level 3s; 26 level 2s; and 3 level 1s).

If you have any questions about responses related to the PACS upgrade, please contact Security Management Division Director Tami Franklin at (202) 564-9218. If you have questions about responses related to contracting, please contact Special Assistant to the Director of OAM Lisa Maass at (202) 564-2498.

Appendix E

Distribution

Office of the Administrator
Deputy Administrator
Assistant Administrator for Administration and Resources Management
Principal Deputy Assistant Administrator for Administration and Resources Management
Chief Financial Officer
Deputy Chief Financial Officer
Director, Office of Budget, Office of the Chief Financial Officer
Director, Office of Human Resources, Office of Administration and Resources Management
Agency Follow-Up Coordinator
General Counsel
Deputy General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Education
Audit Follow-Up Coordinator, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of Administration and Resources Management