

# EVALUATION REPORT

## IMPROVEMENT IS NEEDED IN SBA'S SEPARATION CONTROLS AND PROCEDURES





## EXECUTIVE SUMMARY

Report 15-12

May 26, 2015

### IMPROVEMENT IS NEEDED IN SBA'S SEPARATION CONTROLS AND PROCEDURES

#### What OIG Reviewed

Our objective was to determine the effectiveness of the Small Business Administration's (SBA) controls over separated personnel.<sup>1</sup> Prior external reviews of SBA's Information Technology (IT) security controls indicated recurring, systemic issues, including numerous instances of system access not being deactivated within 24 hours of separation.

We interviewed SBA program officials to gain a high-level understanding of the separation process, tested and analyzed separated employees' separation documents to determine compliance with existing SBA Standard Operating Procedures (SOPs), and tested and analyzed SBA's network accounts for SBA personnel. Further, we reviewed our results with related program offices to confirm our understanding of separation control issues and causes for non-compliance.

#### What OIG Found

SBA's separation guidance—which requires that personnel's IT network accounts be deactivated within 24 hours—is intended to safeguard SBA's network and facilities from breaches. However, we found that SBA's current controls do not accomplish this goal.

Specifically, our analysis of network accounts identified active accounts of 73 personnel that should have been deactivated. We brought this to the attention of the Office of the Chief Information Officer (OCIO), who disabled the accounts. Additionally, we identified two security incidents in which separated employee accounts were accessed after the employee's separation date.

These issues occurred due to non-compliance with existing procedures. For example, we reviewed a judgmental sample of 57 paper-based separation checklists, which are used to terminate network access and collect Federal property from separated employees. However, we found that less than half of the forms—46 percent—were

correctly completed, and 19 percent could not be found. SBA staff explained that the checklist was time-consuming and lengthy and was not always completed properly.

We also found multiple errors in the manner that contracting officer's representatives (CORs) carried out contractor separations, and also noted that SBA did not have formal procedures on how to deactivate and terminate intern and volunteer accounts.

In order for SBA to properly safeguard its systems, SBA will need to strengthen its separation controls.

#### OIG Recommendations

The Office of Human Resources Solutions (OHRS) should identify ways to simplify tasks relating to the separation cycle and reinforce the importance of completing the separation checklist. Additionally, OCIO should improve its network monitoring, clarify policies, and further investigate the two identified security incidents. Finally, the Chief Acquisition Officer should reinforce CORs' oversight and monitoring procedures.

#### Agency Comments

On May 1, 2015, management submitted formal comments. SBA generally concurred with our findings and recommendations.

#### Actions Taken

SBA has already begun to issue periodic reminders reinforcing the importance of completing the separation form and considered ways to simplify the separation process. Management plans to update policies for contractors to mirror those for employees and update policies to reflect current practice for interns and volunteers. OCIO additionally plans to investigate the two security incidents and reinforce its email access policy.

<sup>1</sup> Personnel include SBA employees, contractors, interns, and volunteers.



**U.S. SMALL BUSINESS ADMINISTRATION  
OFFICE OF INSPECTOR GENERAL  
WASHINGTON, D.C. 20416**

---

**Final Report Transmittal**  
Report Number: 15-12

**DATE:** May 26, 2015

**TO:** Maria Contreras-Sweet  
Administrator

Matthew Varilek  
Chief Operating Officer, Office of the Chief Operating Officer

**SUBJECT:** *Improvement is Needed in SBA's Separation Controls and Procedures*

This report presents the results of our evaluation of the Small Business Administration's (SBA) separation controls and procedures. The objective of our evaluation was to determine if SBA was terminating employee, contractor, intern, and volunteer access to IT systems after those individuals ended their employment with SBA.

The report contains six recommendations that SBA agreed to implement. Please provide us within 90 days your progress in implementing the recommendations.

We appreciate the courtesies and cooperation extended to us during this evaluation.

/s/  
Troy M. Meyer  
Assistant Inspector General for Auditing

## Table of Contents

---

Introduction.....	1
Prior Work.....	1
Objectives.....	2
Finding 1: Information System User Accounts Not Consistently Terminated for Separated Personnel.....	3
Employee Separation .....	3
Contractor Separation .....	4
Intern and Volunteer Separation .....	4
Network Account Removal Procedures .....	5
Recommendations to OHRS.....	5
Recommendations to OCIO.....	5
Recommendations to Chief Financial Officer/ Chief Acquisition Officer.....	5
Recommendations to Chief Operation Officer .....	5
Analysis of Agency Response.....	5
Appendix I: Scope and Methodology.....	8
Use of Computer-Processed Data.....	8
Review of Internal Controls.....	8
Nature of Limited or Omitted Information .....	9
Prior Coverage .....	9
Appendix II: Open Recommendations Relating to Separation Controls.....	10
Appendix III: Agency Comments.....	11

## Introduction

---

Employee, contractor, volunteer, and intern (“personnel”) separations from SBA include both voluntary separations, such as resignations and retirements, and involuntary separations, such as dismissals. While varying procedures govern SBA personnel’s separation, a primary focus of these Standard Operating Procedures (SOPs) is to ensure that Government property, such as an employee’s personal identity verification (PIV) card, is returned, and that within 24 hours, separated personnel do not have continued access to SBA facilities and information systems.<sup>2</sup> In order to ensure that only authorized users have access to SBA’s network, the Office of the Chief Information Officer (OCIO) performs additional access controls, including a bi-annual validation of information system accounts, disabling accounts after 60 days of inactivity, and terminating accounts after 120 days of inactivity.<sup>3</sup>

These separation controls are essential to protecting SBA’s physical assets, information systems and sensitive data. In addition to revoking system access, separation controls ensure that identification badges are promptly returned, and that employees return Government property, resolve outstanding debts and receive post-employment briefings.

Because employee separations occur in all of SBA’s program offices, these program offices need to work closely in coordination with OCIO and the Office of Human Resources Solutions (OHRS). According to SBA policy, individual program offices should work with their employees to complete SBA’s separation checklist (Form 78)—which includes multiple steps, such as collecting PIV cards and giving security debriefings.<sup>4</sup> OHRS then receives the completed checklist, and administers appropriate payroll transactions. As required by the COR appointment letter, the COR collects separated contractors’ PIV cards and terminates their record in USAccess. Finally, for all personnel, OCIO deactivates all separating personnel’s network account access, thereby ensuring that only authorized accounts are active.

### Prior Work

The Office of Inspector General (OIG) initiated this evaluation of SBA’s separation clearance process because prior audits noted that user accounts were not being disabled or terminated in accordance with established guidance for separated employees and contractors.

In the *Fiscal Year (FY) 2013 SBA Financial Statement Audit*, OIG’s independent public accountant (IPA) identified 20 employees that retained access to SBA’s network after their separation. In FY 2014, the IPA’s financial statement audit reported eight accounts of former SBA employees that were still accessible after their separation date. One of these accounts belonged to a former senior executive. Access to this account after separation did not receive prior managerial approval. As a result of our prior work, OIG has four outstanding recommendations to correct SBA’s separation process and reconcile network accounts, which have all surpassed SBA’s agreed-upon implementation date. The related audit reports and their corresponding recommendations are presented in Appendix II.

---

<sup>2</sup> SBA SOP 34 00, *Separation Clearance*, prescribes the responsibilities and procedures for the clearance of all outstanding property obligations and financial indebtedness to the Agency prior to an employee’s separation.

<sup>3</sup> SBA SOP 90 47 3, *Information System Security Program*, establishes policies and procedures for ensuring an adequate level of information security for all unclassified information, transmitted, stored or disseminated on the Agency’s information systems, including access controls.

<sup>4</sup> SBA SOP 34 00, *Separation Clearance*, prescribes policy and procedures for separating employees including deactivating their network accounts and collecting their PIV cards.

## **Objectives**

Our objective was to determine if SBA was terminating employee, contractor, intern, and volunteer access to IT systems after those individuals ended their employment with SBA.

## Finding 1: Information System User Accounts Not Consistently Terminated for Separated Personnel

In order to prevent unauthorized access and misuse of SBA systems after an employee separates, OCIO deactivates information system user accounts within 24 hours. This makes an account inactive, but does not delete the account from the system. In addition, SBA's SOPs require OCIO to deactivate an account if it is inactive for 60 days, and to terminate it—removing it from the system— if it is inactive for 120 days. Every employee, contractor, intern, or volunteer account that is not timely deactivated from SBA's systems increases the risk of unauthorized access to SBA's systems and related data.

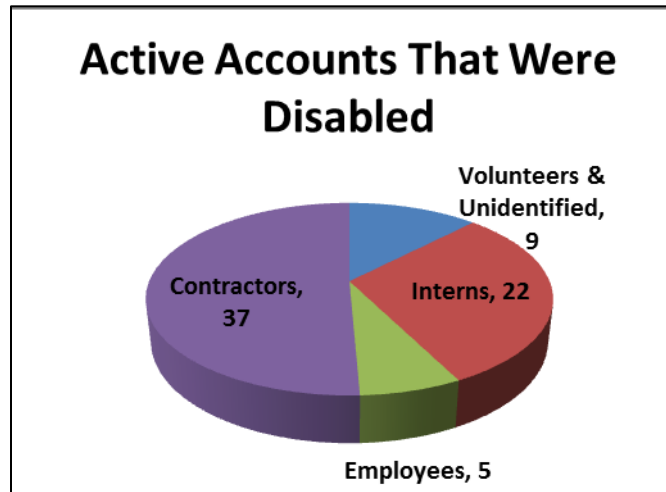
We reviewed all 4,077 active network accounts at the time of our review. We found that 73 accounts were active after the employees' or contractors' separation, or no longer required access to the network. OCIO subsequently terminated these accounts as a result of this review.<sup>5</sup> Of these, 5 were employees, 37 were contractors, 22 were interns, and 9 were volunteers or unidentified.<sup>6</sup> These accounts dated back to 2006.

### Employee Separation

First, we found that SBA did not deactivate and terminate network accounts for all separated employees. Of the 73 open network accounts that should have been disabled or terminated, 5 belonged to employees. These accounts should have been deactivated within 24 hours of an employee's separation and terminated 120 days after separation.

Second, we also found that, even when SBA did deactivate accounts of separated employees, it was not always done timely. We reviewed the accounts of all separated employees from October 1, 2013 to June 27, 2014. Of the 440 accounts in this sample, we found that SBA did not deactivate 8 accounts within 24 hours of separation.

These issues occurred because the separation checklist, Form 78, which guides the separation process, was not consistently followed. In preparation for employee separation, employees and their supervisors are required to complete the checklist, which outlines the numerous steps that must be accomplished prior to separation. However, of our sample of 57 checklists, 11 could not be located, and 20 were incomplete. Also, 17 checklists in the sample did not indicate that the employee had their network access terminated.<sup>7</sup>



<sup>5</sup> We reconciled the existing network accounts against active employees and contractors and found that 152 accounts were not included as belonging to a current employee or contractor who was required to complete the annual computer security awareness training. We requested further analysis by OCIO, who subsequently disabled 73 accounts out of 152.

<sup>6</sup> We could not determine the type of personnel (i.e. employee, contractor, etc.) for three accounts because we were unable to locate the account owner's manager, supervisor, or director.

<sup>7</sup> We also noted that SBA's Office of Disaster Assistance, which processes its own separations, used an outdated version of the separation checklist, which did not include all the items on the new form.

We spoke to OHRS regarding how the checklist entails many time-consuming steps; it is not always followed, and is therefore ineffective in controlling employee separations. OHRS noted that employees retiring under structured separation programs (such as voluntary separation incentive payments) were much more likely to complete the checklist

Because SBA did not always deactivate network accounts within the required 24-hour period, SBA's risk for security breaches was increased. We identified six instances where an employee's account was accessed after their separation—two of which were accessed 11 and 13 days after the employee's separation without their managers' knowledge.<sup>8</sup> We provided these accounts to OCIO for further review.

The remaining four accounts were accessed by the managers or the director so that they could retrieve documentation, such as emails relating to SBA loans sent directly to former employee's SBA email account, or for administrative reasons. In all four cases, the manager or director failed to request the required authorization from the chief information security officer, Office of General Counsel, and chief human capital officer, as required by SBA policy.<sup>9</sup>

### **Contractor Separation**

Of the 73 open network accounts that should have been deactivated and terminated, 37 belonged to contractors. OCIO requires contractor accounts to be disabled within 24 hours of separation or after 60 days of inactivity, and terminated after 120 days of inactivity. We also identified five PIV cards of separated contractors that were not terminated from the USAccess system, which is used to monitor PIV cards, in accordance with SBA policy.<sup>10</sup> An active PIV card can allow access to SBA facilities.

This violation of policy occurred because CORs had insufficient guidance to consistently carry out their responsibilities. The COR serves as an integral component in ensuring that network access procedures for contractors are handled effectively. Current SOPs require the COR to ensure that PIV cards are collected, system access is cancelled, and security clearances are updated upon contractor termination. The COR is also responsible for notifying OCIO if the contractor no longer requires network access. However, the main contracting guidance, SOP 00 11, *Acquisition Standard*, has no checklist or formal documentation to guide the COR for monitoring or separating contractors. Without this guidance, CORs may not consistently inform OCIO of employment status changes or necessary account removals.

### **Intern and Volunteer Separation**

Of the 73 open network accounts that should have been deactivated and terminated, 22 belonged to interns and 6 belonged to volunteers. This occurred because when volunteers and interns separate, SBA has no required overarching record of separation, such as a separation checklist.

---

<sup>8</sup> A security incident is an event determined to be a deliberate or accidental subversion of the confidentiality, integrity, or availability of information.

<sup>9</sup> SBA SOP 90-49.1, *Appropriate Use of SBA's Automated Information Systems* (December 1, 2008).

<sup>10</sup> USAccess is a General Services Administration system to sponsor, enroll, issue and maintain a PIV card for each applicant, and includes built-in workflow processes at every stage of the credentialing process.



## **Network Account Removal Procedures**

Finally, of the 73 open network accounts that should have been deactivated or terminated, 54 accounts were never accessed. This occurred due to a gap in OCIO's oversight controls. OCIO performs reviews of network accounts to ensure active accounts represent authorized users. These reviews should have deactivated or terminated these accounts. Consequently, our review found that this process did not sufficiently consider accounts that have never been accessed and disable those accounts.

### **Recommendations to OHRS**

1. We recommend that SBA reinforce the importance of completing the Form 78 and consider ways to simplify the completion cycle.

### **Recommendations to OCIO**

2. We recommend the Chief Information Officer further investigate the two security incidents, where separated employee's accounts were logged into after separation, to determine if a reportable condition existed in accordance with United States Computer Emergency Readiness Team (US CERT) guidance.
3. We recommend that the Chief Information Officer ensure its network oversight includes enabled network accounts which have never been accessed.
4. We recommend the Chief Information Officer clarify email access policies as defined in SOP 90 49.1.

### **Recommendations to Chief Financial Officer/ Chief Acquisition Officer**

5. We recommend the Chief Financial Officer/Chief Acquisition Officer revise guidance to require the COR to monitor contractor status and provide a standardized method to do so. This guidance should reinforce COR responsibilities for monitoring a contractor's system or network access, identification card receipt and return, SBA separation date, system or network deactivation and security notification date.

### **Recommendations to Chief Operation Officer**

6. We recommend the Office of Chief Operating Officer's Office of Administrative Services establish separation criteria for interns and volunteers. The criteria should include network removal procedures and timely return of SBA identification cards.

## **Analysis of Agency Response**

SBA management provided formal comments, which are included in their entirety in Appendix III. The following provides a summary of management's comments and the actions necessary to close the report.

Agency management agreed with five of six recommendations and partially agreed with one. Management partially disagreed with our recommendation that the Office of the Chief Administrative Officer establish separation criteria for interns and volunteers over the inclusion of network removal procedures. Management states that network removal procedures fall under the Office of Chief information Officer, which is responsible for ensuring that separations will be properly addressed on the Network.

## **Summary of Actions Necessary to Close the Report**

### **1. Reinforce the importance of completing the Form 78 and consider ways to simplify the completion cycle.**

OHRS agreed with the recommendation and has already begun to issue periodic notices to remind supervisors, managers, and employees of their responsibility to complete SBA Form 78. OHRS plans to expand its efforts to reinforce the importance of completing Form 78 through monthly conference calls and by requesting attendance to participate in the program offices' weekly/monthly managers' meetings and reinforcing the need to have SBA Form 78 completed by managers in a timely manner. The agency stated it will alert managers that they can be held accountable for failure to ensure forms are completed and have an adverse impact on their annual performance review. Additionally, OHRS will give prior notice to departing employees that their final lump-sum payment will be held until the form is completed. OHRS stated it was also working to simplify the completion cycle. This recommendation is considered closed.

### **2. Further investigate the two security incidents, where separated employees' accounts were logged into after separation, to determine if a reportable condition existed in accordance with United States Computer Emergency Readiness Team (US CERT) guidance.**

OCIO agreed with the recommendation and stated that it will investigate the two security incidents to determine if a reportable condition existed in accordance with United States Computer Emergency Readiness Team (US CERT) guidance. OCIO proposed implementing this recommendation by September 1, 2015. This recommendation can be closed upon OCIO providing evidence that it has investigated the two security incidents.

### **3. Ensure its network oversight includes enabled network accounts which have never been accessed.**

OCIO agreed with the recommendation and stated that it has issued a recertification policy in which every account is reviewed and any account not accessed in the previous 60 days is disabled. This recommendation can be closed upon OCIO providing evidence that it has issued a policy requiring accounts not accessed in 60 days to be disabled and evidence that the control is operating effectively.

### **4. Clarify email access policies as defined in SOP 90 49.1.**

OCIO agreed with the recommendation and stated that it will review the SOP to see if clarification is needed and issue bi-annual notices to all employees clarifying email access policies. OCIO proposed implementing this recommendation by October 1, 2015. This recommendation can be closed upon OCIO providing evidence that the SOP has been reviewed and bi-annual notices to employees are being sent.

- 5. Revise guidance to require the COR to monitor contractor status and provide a standardized method to do so. This guidance should reinforce COR responsibilities for monitoring a contractor's system or network access, identification card receipt and return, SBA separation date, system or network deactivation and security notification date.**

The Chief Financial Officer/Chief Acquisition Officer agreed with the recommendation and plans to require contractors to follow the same procedures as employees effective October 1, 2015. This recommendation can be closed upon the Chief Financial Officer/Chief Acquisition Officer providing evidence that guidance to the COR has been updated to require contractors to follow the same separation procedures as employees .

- 6. Establish separation criteria for interns and volunteers. The criteria should include network removal procedures and timely return of SBA identification cards.**

The Office of Chief Administrative Officer (OCAO) partially agreed with the recommendation. OCAO partially disagreed with the inclusion of network removal procedures as those fall under OCIO. OCAO stated that they are currently updating the SOP, and will expand the section "Who Needs a PIV Credential?" to include interns, and will include volunteers and interns in the PIV credential termination process section. OCAO proposed implementing this recommendation by September 30, 2015. This recommendation can be closed upon OCAO providing evidence that the SOP has been updated.

## **Appendix I: Scope and Methodology**

---

We conducted this evaluation in accordance with the Council of Inspectors General on Integrity and Efficiency Standards for Inspection and Evaluations. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our objectives.

As a result of previously issued and unresolved recommendations, OIG initiated an evaluation with the overall objective of determining the effectiveness of controls over separated employees and contractors. This evaluation primarily focused on (1) separation clearance forms being completed to protect SBA by returning agency badges and SBA property, (2) SBA network accounts being timely revoked, and (3) related risks resulting from SBA network accounts being accessed after the personnel's separation date.

To accomplish these objectives we:

- interviewed key SBA personnel to gain a high-level understanding of the separation process;
- obtained and examined a sample of employee separation checklists (Form 78) and contractor computer access clearance/security forms (Form 1228);
- reconciled 440 employee separations to network accounts and identification cards;
- identified 152 employees, contractors, interns, and volunteers out of over 11,000 network accounts that were not identified as current SBA personnel;
- identified and analyzed control issues by comparing separated employees and contractors with SBA's network access listing, SBA PIV cards, other SBA identification cards, and the computer security awareness training listing; and
- reviewed our results with OCIO personnel and related program offices to further understand root causes for separation control non-compliance.

Our scope encompassed separations and supporting documentation from October 1, 2013 to June 30, 2014.

### **Use of Computer-Processed Data**

We relied on the data prepared by the SBA program office that was generated from several SBA databases. Data in these databases are in operation and used by SBA offices. Auditors performed several checks on the data and believe the information is reliable for the purposes of this evaluation.

### **Review of Internal Controls**

Our evaluation encompassed an assessment of the effectiveness of SBA's existing separation controls. To assess the effectiveness of these controls, we evaluated SBA practices against SOPs related to the processing and account management of separated personnel. Specifically, our review determined whether employee separations complied with SBA's separation clearance SOP. For contractors, we evaluated compliance with criteria in SBA's procurement SOPs. We also determined whether network and PIV accounts of separated personnel were disabled and terminated in accordance with SBA's Information System Security Program and PIV credentials SOPs.

## **Nature of Limited or Omitted Information**

No information was omitted due to confidentiality or sensitivity, nor were there limitations to information on this evaluation.

## **Prior Coverage**

*Small Business Administration—Office of Inspector General Reports*

Audit Report 15-02, *Independent Auditors' Report on the SBA's FY 2014 Financial Statements* (November 17, 2014).

Audit Report 14-04, *Independent Auditors' Report on the SBA's FY 2013 Financial Statements* (December 16, 2013).

Audit Report 13-04, *Independent Auditors' Report on the SBA's FY 2012 Financial Statements* (November 14, 2012).

Audit Report 12-15, *Weaknesses Identified During the FY 2011 Federal Information Security Management Act Review* (July 16, 2012).

## **Appendix II: Open Recommendations Relating to Separation Controls**

There are four open recommendations to correct SBA's separation process and reconcile network accounts, which have all surpassed SBA's agreed-upon corrective action due date. The related audit reports and their corresponding recommendations can be found below.

Audit Report 15-02 – *Independent Auditors' Report on the SBA's FY 2014 Financial Statements* and  
Audit Report 14-04 – *Independent Auditors' Report on the SBA's FY 2013 Financial Statements*

- **Recommendation:** The Chief Information Officer coordinate with SBA program offices to improve SBA 's administration of logical system access by taking the following actions:
  - Implement an effective off-boarding process and verify periodically that controls to remove logical access for separated employees from SBA systems are implemented and operating as designed;
  - Establish a process for the identification and removal of separated contractors in order to help ensure that access is timely removed upon contractor separation; and
  - Remove access to the general support systems and major applications (including development and test environments) timely when terminated employees and contractors are identified.

Audit Report 13-04 – *Independent Auditors' Report on the SBA's FY 2012 Financial Statement*

- **Recommendation:** The Chief Information Officer coordinate with SBA program offices to develop and implement procedures for user access termination to ensure that access for terminated or transferred personnel is removed from systems in a timely manner.

Audit Report 12-15 – *Weaknesses Identified During the FY 2011 Federal Information Security Management Act Review*

- **Recommendation:** The Chief Information Officer perform periodic recertification reviews of end-users in agency general support systems to ensure that users are authorized and have current access privileges. Alternatively, design compensating controls for recertification for end-users of general support systems.

## Appendix III: Agency Comments

---



U.S. SMALL BUSINESS ADMINISTRATION  
WASHINGTON, D.C. 20416

May 1, 2015

Mr. Troy M. Meyer  
Assistant Inspector General for Auditing  
U.S. Small Business Administration  
409 Third Street, S.W.  
Washington, DC 20416

Dear Mr. Meyer:

Thank you for the opportunity to review the draft evaluation report entitled *Improvement is Needed in SBA's Separation Controls and Procedures*. We have reviewed the referenced report and its recommendations to the Chief Administrative Officer, Chief Financial Officer, Chief Information Officer, and the Chief Human Capital Officer.

### **IG Recommendations to OHRS**

1. We recommend that SBA reinforce the importance of completing the Form 78 and consider ways to simplify the completion cycle.

**SBA Response:** We agree with the recommendation. We have already begun to issue periodic notices in the SBA Daily reminding supervisors, managers and employees of their responsibility to complete the SBA Form 78. OHRS plans to expand the efforts to reinforce the importance of completing the Form 78 through monthly AO conference calls and by requesting attendance to participate in the Program Offices' weekly/monthly managers' meetings and reviewing/reinforcing the need to have the SBA Form 78 completed by managers in a timely manner. The agency can hold managers accountable for failure to ensure forms are completed by noting this as a significant exception to the manager's critical element for "People Responsibilities." Alerting managers to the fact that non-compliance can have a direct, adverse impact on their annual performance review should encourage them to complete the task. Additionally, giving prior notice to departing employees that their final lump-sum payment will be held until the form is completed should encourage them to follow-up with their manager to ensure the form is completed as well. We are also working to simplify the completion cycle.

### **IG Recommendations to OCIO**

2. We recommend the Chief Information Officer further investigate the two security incidents, where separated employees' accounts were logged into after separation, to determine if a reportable condition existed in accordance with United States Computer Emergency Readiness Team (US CERT) guidance.

**SBA Response:** We agree with the recommendation. OCIO will investigate the two security incidents to determine if a reportable condition existed in accordance with United States Computer Emergency Readiness Team (US CERT) guidance by September 1, 2015.

3. We recommend that the Chief Information Officer ensure its network oversight includes enabled network accounts which have never been accessed.

**SBA Response:** We agree with the recommendation. OCIO has issued a Recertification Policy in which every account is reviewed and any account not accessed in the previous 60 days is disabled.

4. We recommend the Chief Information Officer clarify email access policies as defined in SOP 90 49.1.

**SBA Response:** We agree with the recommendation. OCIO will review the SOP by October 1 to see if clarification is needed. OCIO will issue bi-annual notices to all employees clarifying email access policies.

#### **Recommendations to Chief Financial Officer/Chief Acquisition Officer**

5. We recommend the Chief Financial Officer/Chief Acquisition Officer revise guidance to require the COR to monitor contractor status and provide a standardized method to do so. This guidance should reinforce COR responsibilities for monitoring a contractor's system or network access, identification card receipt and return, SBA separation date, system or network deactivation and security notification date.

**SBA Response:** We agree with the recommendation. Effective October 1, 2015, contractors will follow the same procedures as employees, utilizing the SBA Form 78.

#### **Recommendations to Chief Administrative Officer**

6. We recommend the Office of Chief Administrative Officer's Office of Administrative Services (Facilities, Safety, and Security Services) establish separation criteria for interns and volunteers. The criteria should include network removal procedures and timely return of SBA identification cards.

**SBA Response:** We partially agree with the recommendation. The Standard Operating Procedure 00 07, Homeland Security Presidential Directive – 12 (HSPD – 12) Personal Identity Verification (PIV), currently states that volunteers must obtain PIV Credentials (cards) (see Page 5); however, it does not specifically address volunteers in the subsequent section on PIV termination.

At present, any interns or volunteers with SBA longer than 6 months, who possess PIV cards, follow the same procedures for PIV card termination as employees and contractors. Upon revision of the SBA Form 78, that will be the vehicle for our office to use to document and authorize receipt of the PIV card during the separation/exit process.

We are currently updating the SOP, and will do the following:

- Chapter 1, Section 2 - Expand the definition to include the term "interns". OCAO will work with OHRS on the definition, since most interns are not with the Agency longer than 6 months (which is the requirement for a PIV card – see Page 7).
- Chapter 4, Section 10: Expand the language on PIV termination on page 20 to specifically include volunteers and interns, timely return of the PIV cards (and/or SBA temporary IDs) to SBA, as well as any other situation for which a PIV card will be terminated (i.e., lack of use).



Our partial disagreement with this recommendation to the Office of the Chief Administrative Officer, relates to the fact that network removal procedures fall under the Office of the Chief Information Officer. OCIO will ensure that separations will be properly addressed on the Network. Once PIV cards are returned, Administrative Services ensures that the PIV cards are destroyed and the associated record has been terminated in GSA's system.

Respectfully,

Matt Varilek  
Chief Operating Officer

cc:  
Bridget Bean  
Donna Butler  
Don Sanders  
Renee Macklin  
Tami Perriello