

SYSTEM ACCESS BY CONTRACTORS WITHOUT SECURITY CLEARANCES

Report Number 09-07

Date Issued: January 26, 2009

**Prepared by the
Office of Inspector General
U. S. Small Business Administration**



U.S. Small Business Administration
Office Inspector General

Memorandum

To: Christine Liu
Chief Information Officer
/s/ original signed

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: System Access By Contractors Without Security Clearances
Report No. 09-07

Date: January 26, 2009

This report supplements our evaluation of the Federal Information Security Management Act (FISMA) implementation for Fiscal Year 2008. The Office of Inspector General (OIG) is required to annually assess SBA's compliance with FISMA in accordance with specific reporting instructions issued by the Office of Management and Budget (OMB).¹ During the course of our FY 2008 FISMA review, we determined that SBA did not consistently ensure that contractors were properly vetted prior to granting them access to sensitive SBA systems and data. This vulnerability was not consistently reported and tracked in SBA's Plan of Action and Milestones (POA&M).

In order to assess security controls over contractor access, we reviewed SBA access requirements outlined in Standard Operating Procedure (SOP) 90 47 2. We also requested the names of contractors with access to all hosted applications² on the following 10 systems:

[FOIA ex. 2

¹ Memorandum 08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

² These included applications in both production and test environments.

]

We compared contractor names to Agency and OIG records and interviewed the appropriate Agency representatives to determine whether background investigations and clearances had been completed for contractor staff. To determine whether SBA appropriately identified and corrected vulnerabilities involving unauthorized contractor access, we reviewed OMB Memorandum M-04-25 requirements and the Agency's POA&M quarterly reports for FY 2008. Our review was conducted in accordance with the *Government Auditing Standards* as prescribed by the Comptroller General of the United States.

BACKGROUND

OMB Circular A-130 requires Federal agencies to screen individuals applying for access to government data and systems based on the level of risk presented by their access. SOP 90 47 2 classifies all SBA data as sensitive and requires all contractor personnel to undergo background investigations. In addition, contractor personnel occupying positions designated as critical-sensitive cannot be given access to sensitive data until an appropriate security clearance has been granted. SBA requires that SBA Form 1228, *Computer Access Clearance/Security*, be used to request all network account access for new contractor employees.

Currently, the Contracting Officer's Technical Representatives (COTRs) assigned to each program office are responsible for identifying all contractor personnel who require access to SBA systems and records.³ The COTR submits system access requests to the OIG Security Office, which performs the preliminary background checks. After the OIG completes the background check, the signed access request is sent to the appropriate staff for processing. The contractor may then be granted temporary system access pending the completion of the full clearance process.

³ SBA Procedural Notice 9000-1684, *SBA Form 1228 Process*.

RESULTS

SBA Granted System Access to Contractors Who Lacked the Required Background Investigations and Security Clearances

Contractor employees were granted access to sensitive SBA systems and data without evidence of completed background investigations and security clearances, as required by SOP 90 47 2. Of the 10 systems reviewed, we identified 6 that were accessed by contractors, who did not have the required background investigations and clearances:

- [FOIA ex. 2] – Five of seven contractors were found to occupy sensitive positions, such as Systems Administrator, without background investigations and subsequent clearances. In some cases, the contractors had access to both production and test data.
- [FOIA ex. 2] – One of four contractors lacked evidence of a background investigation and clearance.
- [FOIA ex. 2] – All 33 contractors lacked a background investigation and clearance.
- [FOIA ex. 2] – Two of nine contractors did not have evidence of a background investigation and clearance.
- [FOIA ex. 2] – All 18 contractors lacked a background investigation and clearance.
- [FOIA ex. 2] – One of three contractors did not have an SBA background investigation and clearance.

Although SBA procedures require a background investigation and SBA authorization for all contractors accessing SBA data, not all COTRs were aware of this requirement, and instead, relied on vendors to clear their own employees for access. For example, the COTRs for [FOIA ex. 2] and the [FOIA ex. 2] were unaware of the SBA background investigation and clearance requirements until the OIG made inquiries. As a result, critical and sensitive SBA systems and data (including Personally Identifiable Information) were at risk of unauthorized access and subsequent waste, loss, and misuse.

Only four of the six systems we identified were reported as having contractor access-related vulnerabilities on SBA's POA&M. Access vulnerabilities

associated with [FOIA ex. 2] and [FOIA ex. 2] were not reported. The POA&M also identified an additional five systems as having vulnerabilities associated with contractor access, which, with the exception of [FOIA ex. 2], we did not review. These systems included the:

- [FOIA ex. 2];
- [FOIA ex. 2]⁴;
- [FOIA ex. 2];
- [FOIA ex. 2]; and
- [FOIA ex. 2]

SBA Did Not Consistently Report Vulnerabilities Involving Unauthorized Contractor Access

OMB Memorandum M-04-25 requires agencies to prepare a POA&M for all programs and systems where an IT security vulnerability has been found and to brief OMB. Program officials are further required to update the Agency's Chief Information Officer (CIO) on the status of their progress in addressing the vulnerabilities by reporting this information in the POA&M at least quarterly so that the CIO can monitor agency-wide remediation efforts. Additional Federal guidance requires system owners to perform timely corrective actions to address the vulnerabilities.⁵

Despite these requirements, system owners did not consistently identify and/or address identified vulnerabilities associated with contractor access to sensitive SBA systems and data. A review of quarterly POA&Ms for FY 2008 disclosed that unauthorized contractor access to the 11 systems on the POA&M were not consistently reported as vulnerabilities and that the vulnerabilities were not consistently prioritized and remediated. A summary of how these vulnerabilities were reported is shown in the following table.

⁴ Our review of [FOIA ex. 2] did not disclose any employees with background investigation/clearance issues. However, the quarterly POA&Ms reported a vulnerability.

⁵ National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Table 1. Summary of POA&M Vulnerabilities Involving Unauthorized Contractor Access

System ⁶	Disclosure and Rating of Vulnerability			
	POA&M 1 st Quarter 2008	POA&M 2 nd Quarter 2008	POA&M 3 rd Quarter 2008	POA&M 4 th Quarter 2008
[FOIA ex. 2]	Not Reported	Not Reported	Not Reported	Low
[FOIA ex. 2]	Not Reported	Not Reported	High	High
[FOIA ex. 2]	Low	Low	Not Reported	Not Reported
[FOIA ex. 2]	Not Reported	Not Reported	Not Reported	Not Reported
[FOIA ex. 2]	Not Reported	Not Reported	Not Reported	Not Reported
[FOIA ex. 2]	Reported, but not ranked	Reported, but not ranked	Reported, but not ranked	Reported, but not ranked
[FOIA ex. 2]	Medium	Medium	Medium	Medium
[FOIA ex. 2]	Medium	Medium	Medium	Medium
[FOIA ex. 2]	High	High	Vulnerability Remediated	Vulnerability Remediated
[FOIA ex. 2]	Not Reported	Not Reported	Medium	Medium
[FOIA ex. 2]	Not Reported	Not Reported	High	High

Source: OCIO quarterly POA&M reports for FY 2008.

For example, SBA did not report a vulnerability related to unauthorized contractor access to [FOIA ex. 2] in the first two quarters of 2008, but subsequently reported it as a high-risk vulnerability in the last two quarters of 2008. Further, vulnerabilities related to contractor access were sometimes rated as a high-risk, and other times as medium- or low-risk.

Inconsistencies in reporting vulnerabilities associated with contractor access were due to several factors. First, contractors performing Certification and Accreditation reviews and security self-assessments of the various systems did not consistently identify improper contractor access as a vulnerability. Secondly, because OCIO did not provide guidance on how such vulnerabilities should be rated, ratings varied. Finally, in preparing the POA&M, OCIO staff did not identify inconsistencies in how the vulnerabilities were being reported and rated, and allowed vulnerabilities to be dropped without appropriate documentation.

⁶ Includes general support systems, such as [FOIA ex. 2] and the [FOIA ex. 2].

RECOMMENDATIONS

We recommend the Chief Information Officer:

1. Require system owners to confirm that all contractor personnel with access to sensitive systems and data have background investigations and clearances commensurate with SBA policy.
2. Immediately suspend system access for any contractors who do not comply with SBA background investigation and security clearance policies.
3. Work with the Office of Management and Administration to notify COTRs of SBA's system access requirements related to contractor personnel.
4. Require that the C&A reviews and the security self-assessments determine whether contractor employees have the required background investigations and clearances for system access.
5. Develop guidance on how contractor access vulnerabilities should be rated and reported in the quarterly and annual POA&M reports.
6. Require documentation justifying removal of previously reported vulnerabilities from the POA&M.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On December 16, 2008, we provided a draft of this report to SBA for comment, and on January 23, 2009, we received written comments from the Chief Information Officer which are contained in their entirety in Appendix I.

While the OCIO agreed to take action on the recommendations, we found that the proposed actions to be taken in response to Recommendations 1, 2, 4, 5 and 6 were not sufficient to fully address the related findings. We consider the OCIO response to Recommendation 3 to be sufficient to mediate the related finding.

We recognize the actions taken by the OCIO staff to address issues that the audit team brought to their attention and look forward to resolution of all findings and implementation of all recommendations.

ACTIONS REQUIRED

Because your comments did not fully address Recommendations 1, 2, 4, 5 and 6, we request that you provide a written response by February 20, 2009, providing proposed actions and target dates for implementing the recommendations.

We appreciate the courtesies and cooperation of the OCIO during this audit. If you have any questions concerning this report, please call me at (202) 205-[FOIA ex. 2] or Jeffrey Brindle, Director, Information Technology & Financial Management Group, at (202) 205-[FOIA ex. 2].

Appendix I.



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

Date: January 22, 2009

To: Debra S. Ritt
Assistant Inspector General for Auditing

From: Christine H. Liu [FOIA Ex 6]
Chief Information Officer

Subject: Comments re: System Access by Contractors Without Security Clearances
Project No. 8011

We appreciate the opportunity to review this report. We are sensitive to the need to protect access to SBA data, and plan to work diligently to improve both process and performance in this critical area. As shown below we are taking steps to remediate each of these findings:

- In conjunction with the Office of Management and Administration (M&A) we are reissuing and updating the SBA Procedural Notice to strengthen the language requiring all Contracting Officer Representatives or Technical Representatives (COR/COTR) to ensure that contractors are cleared prior to access to SBA data.
- As a part of reissuing this Procedural Notice, we are revisiting the controls and COTR procedures in the SBA Form 1228 process to ensure that we can audit and verify completion of the process.
- Working closely with both the Office of the Inspector General and M&A we are updating SBA SOP 90.47.2 to clarify and strengthen the controls and procedures required for contractor background investigations and system access.
- Our Certification & Accreditation (C&A) process assesses the NIST SP 800-53 controls relating to contractor clearances and access to data. We are enhancing these controls by rating and identifying vulnerabilities to ensure consistency with our findings.
- Once the vulnerability is identified, the Plan of Action and Milestones (POA&M) process is in place to track and report the vulnerabilities.

OCIO will continue to be an integral part of the check and balances ensuring the protection of SBA data along with the Program Offices responsible for identifying the contractors that must be cleared.