

CONTROLS OVER ACCESS TO EMPLOYEE EMAILS BY SBA MANAGERS

Report No. 08-02
Date Issued: October 19, 2007

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



Memorandum

U.S. Small Business Administration
Office of Inspector General

To: Christine Liu
Chief Information Officer

Date: October 19, 2007

From: Debra S. Ritt
Assistant Inspector General for Auditing
/S/ original signed
Subject: Report on Controls over Access to Employee Emails by SBA Managers

This report identifies the potential risks related to administrative access to employee emails and information system applications by Small Business Administration (SBA) managers, and recommends actions to strengthen controls over email access.

On August 29, 2007, the Inspector General notified you that the Office of Disaster Assistance (ODA) had retrieved emails originating from an employee who was a confidential source to the Office of Inspector General (OIG) and a Congressional committee. The employee's emails were accessed following a Congressional hearing for which the employee, who wished to remain anonymous, had submitted a statement for the congressional record.

We would like to work with you to develop appropriate safeguards to prevent agency review of OIG emails and information system applications. The IG Act of 1978 provides that the identity of Federal employees who raise complaints to the OIG about their employing agency must remain confidential. The Act further prohibits acts of retaliation against employees who submit complaints to the OIG. Management's ability to intercept confidential employee-OIG e-mails raises troubling questions about whether agency employees can confidently and securely bring confidential complaints to the OIG's attention, which undermines these statutory protections.

We met with you in your dual capacity of Chief Information Officer and Chief Privacy Officer to identify your procedures for granting email access and to determine whether your office had authorized the email retrievals. The OIG Investigations Division subsequently conducted interviews of ODA employees which highlighted the ability of ODA management to review employee emails without providing OCIO any justification for such reviews. There was no formal

approval process requiring OCIO to record and release emails to ODA management. The results of our review are summarized below.

RESULTS

SOP 90 47 2, *Automated Information Security (AIS) Program*, states that the Chief Information Officer (CIO) is responsible for the development and implementation of the Agency AIS program. The CIO is also the Chief Privacy Officer, and as such, is responsible for controlling access to emails and system applications. In a February 11, 2005, Office of Management and Budget (OMB) memorandum (M-05-08), agencies were directed to implement actions to safeguard personal information. The memorandum stated, "As is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws and policies, each agency must take appropriate steps necessary to protect personal information from unauthorized use, access, disclosure or sharing, and to protect associated information systems from unauthorized access, modification, disruption or destruction." The OMB memorandum also stated that "[w]hen compliance issues are identified agencies are obligated to take appropriate steps to remedy them."

Based on additional interviews and other information obtained during our review, we determined that the Agency lacked clear written guidance for reviewing employee emails. Standard Operating Procedure (SOP) 90 49, *Appropriate Use of SBA's Automated Information Systems*, specifies that emails "are subject to examination in connection with authorized official Agency reviews (e.g., OIG investigations, audits and inspections, administrative inquiries and reviews, etc.)." However, there is no guidance on when an administrative inquiry and review of emails would be considered "authorized," who would be authorized to review the emails, and when centralized approval would be required.

Our review disclosed that center management accessed an employee's emails without seeking approval from or notifying the CIO. The CIO advised that she and her staff were unaware of the circumstances or actions relating to ODA's review of the emails, and that, as the Agency's Chief Privacy Office, ODA should have obtained her authorization. The CIO also advised that her office had not issued any written guidance on how email reviews should be authorized.

In the absence of controls, such as a centralized authorization process or written guidance for conducting administrative review of employee emails, SBA has no assurance that appropriate safeguards are consistently employed. SBA also lacks the ability to monitor who is reviewing employee emails, the frequency of such reviews, or the purposes of such reviews. Although review of employee emails may be justified in order to determine whether an employee has violated legal or

administrative requirements, or for information technology security purposes, the absence of controls creates an environment where employee emails may be subject to unauthorized access or reviewed for illegitimate purposes.

RECOMMENDATIONS

We recommend that to mitigate potential risks from unauthorized access to emails and system applications, the CIO:

1. Immediately communicate to individuals having system administrator rights that requests for email retrievals must be approved centrally by her office.
2. Revise SOP 90 49 to establish appropriate protocols for conducting administrative inquiries and reviews of employee emails, including identifying the criteria for determining whether an email review would be considered "authorized," and identifying the appropriate authorization levels needed before an administrative review is conducted. The SOP should also define the respective roles of the Chief Privacy Officer, CIO, and Director of Information Security in authorizing access to Agency emails and information system applications.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On September 14, 2007, we provided SBA with a draft of the report for comment. On October 10, 2007, SBA provided its formal response, which is contained in its entirety in Appendix I. SBA agreed with our findings and recommendations and stated that it would prepare an Agency-wide directive by October 19, 2007, that requires all e-mail retrieval requests to be approved centrally by the CIO and Office of General Counsel (OGC). OCIO and OGC will also work jointly to identify criteria and authorization levels required to access Agency user e-mails. Management's comments were responsive to the audit recommendations.

We appreciate the courtesies and cooperation of ODA and OCIO representatives during this review. If you have any questions concerning this report, please call me at (202) 205- [Exemp
2] Jeff Brindle, Director, at (202) 205- [Exemption 2]



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

Appendix 1

Date: October 10, 2007

To: Debra S. Ritt
Assistant Inspector General for Auditing

From: Christine H. Liu [Exemption 5]
Chief Information Officer

Subject: Draft Report on Controls over Access to Employee E-mails by SBA Managers –
Project No. 07-31

In reviewing OIG's draft report on "Controls over Access to employee e-mails by SBA Managers", our office has begun working with the Office of the General Counsel (OGC) on the two OIG recommendations resulting from this report -- for the Agency to put in place policy and measures to mitigate potential risks from unauthorized access to individual user e-mail boxes. We have asked ODA to comment further on the actual audit findings.

A. Recommendation 1: Immediately communicate to individuals having system administrator rights that requests for e-mail retrievals must be approved centrally by his/her office.

SBA Response: The Chief Information Officer (CIO), in conjunction with OGC, will prepare an executive Agency-wide directive for issuance by SBA Deputy or Chief of Staff to require that all e-mail retrieval requests must be submitted to SBA's Chief Information Security Officer (CISO) for approval by the CIO and OGC. This directive will go out by October 19, 2007.

B. Recommendation 2: Revise SOP 90 49 to establish appropriate protocols for conducting administrative inquiries and reviews of employee e-mails, including identifying the criteria for determining whether an e-mail review would be considered "authorized", and identifying the appropriate authorization levels needed before an administrative review is conducted. The SOP should also define the respective roles of the Chief Privacy Officer (CPO), CIO, and Director of Information Security in authorizing access to Agency e-mails and information system applications.

SBA Response:

(1) OCIO and OGC jointly will work on identifying criteria in determining authorized e-mail reviews, and the appropriate authorization levels needed before an administrative e-mail review is conducted.

(2) OCIO will work on incorporating into the SOP 90 49 clear definitions of the respective roles of the CISO, CPO, the CIO and the OGC in authorizing access to Agency user e-mails.

This response addresses authorizing access to e-mail, and not information system applications. We anticipate this policy to be drafted for clearance by October 26, 2007.

cc: OGC - Frank Borchert, General Counsel
OIG - Jeff Brindle, Director
OCIO - David McCauley, CISO
OCIO - Charles McClam, DCIO



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

To: Debra Ritt
Assistant Inspector General for Auditing

From: Herbert L. Mitchell
Associate Administrator for Disaster Assistance

Subject: Draft IG Project No. 07-31 Report

We have reviewed the draft report and agree with both the recommendations made to Christine Liu, Chief Information Officer (CIO), and her responses. We believe that the lack of established policies and procedures on managements' handling of employees' emails resulted in this issue arising in the first place.

Management in the Processing and disbursement Center has indicated that, while attempting to insure that loan applicants' privacy rights were protected, they identified emails from employees without obtaining the authorization from the CIO. Nevertheless, no violations were discovered since the Agency had no policies and procedures in place. This was not done in retaliation for any other activity the employees may have been involved with and management has not acted on any of the information.

Until the Agency develops and issues policies and procedures in regard to the handling of and access to employee emails we have instructed all managers to submit such request to ODA Headquarters for review and a decision by the CIO.

[Exemption 6]

Herbert L. Mitchell

REPORT DISTRIBUTION

<u>Recipient</u>	<u>No. of Copies</u>
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	3
U.S. Government Accountability Office	2