



Office of Inspector General

Report Highlights

Date: May 12, 2008

Title: Lack of Controls over Granting Access to Employee Government E-mail and Computers

Findings: Our review identified internal control concerns regarding supervisors and others access to employee government e-mail and computers. These concerns include the lack of

- a written GAO policy on who may be granted access to employee e-mail and computers,
- written guidance to ISTS Help Desk contractors who receive access requests on when to grant access, and
- a database to track who is given access to employee e-mail and computers.

In the absence of written policies and procedures, we found that ISTS had granted nonemployees access to GAO computers.

We are recommending actions to improve the overall control environment on accessing employee government e-mail and computers.

Recommendations: We make three recommendations to strengthen the controls over access to employee e-mail and computers.

- Develop a written policy regarding supervisors and others access to employee e-mail and computers and inform employees of the policy.
- Establish written procedures for ISTS staff and contractors handling requests to access employee e-mail and computers.
- Expeditiously begin oversight and monitoring of requests to access employee e-mail and computers.



GAO

Accountability • Integrity • Reliability

Memorandum

Date: May 12, 2008

To: Executive Committee

From: Inspector General – Frances Garcia

Subject: Lack of Controls over Granting Access to Employee Government E-mail and Computers

Our review identified internal control concerns regarding the access of supervisors and others to employee government e-mail and computers. These concerns include the lack of

- a written GAO policy on who may be granted access to employee e-mail and computers,
- written guidance to ISTS Help Desk contractors who receive access requests on when to grant access, and
- a database to track who is given access to employee e-mail and computers.

In the absence of written policies and procedures, we found that ISTS had granted nonemployees access to GAO computers.

Background

According to ISTS officials, three units in ISTS receive requests from supervisors and others to access employee e-mail and computers. Two of these units receive requests of a sensitive nature, which go through GAO's Chief Information Officer. The third unit—IST's Help Desk—receives requests directly. Regarding information privacy, GAO Order 0510.2¹ states, "All access to GAO information systems is subject to monitoring; to which all users must affirmatively consent when accessing any system." GAO's network login banner reinforces this point.² However, GAO attorneys told us that supervisors and others access rights have some limits because employees can have some expectation of privacy over personal information, such as doctor calendar appointments and medical information on employees' computers.

¹GAO Order 0510.2, Information Systems Security Policy, September 30, 2004.

² The login banner states that "This system is for official use by U.S. GAO authorized personnel only All activities may be monitored, recorded, or copied by authorized personnel and such information may be provided to law enforcement officials. Use of this system by any user constitutes consent to these conditions."

Lack of Policy and Procedures over Access to Employee E-mail and Computers Raises Control Concerns

According to ISTS officials, GAO has no written policy or internal controls over who may be granted access to employee e-mail and computers. Without such a policy or control, GAO does not have assurance that only appropriate access is being granted or that consistent procedures are being followed. For example, ISTS in early January 2008 granted a deceased employee's spouse direct access to the employee's computer harddrive. The supervisor of the deceased employee had requested that ISTS staff extract the information from the harddrive for the spouse, but ISTS was unable to provide any staff. As a result, the supervisor gave the spouse direct access and asked a team member to be present while the spouse extracted information. In a second case, ISTS allowed a spouse to be present while ISTS staff extracted information from a deceased employee's harddrive.

According to GAO attorneys, because harddrives in government computers could contain sensitive or limited official use information, it was inappropriate for ISTS to provide the spouse (who was not employed by GAO) direct access to the deceased employee's computer. In the second case, it was also inappropriate for the spouse (who was not employed by GAO and a foreign national) to be present while information from a government computer was extracted. GAO attorneys stated an alternative best practice would be to have a spouse or other appropriate next of kin make a written request for access; if approved, have ISTS staff extract the information without the spouse being present and then provide them the extracted personal information.

While ISTS officials told us that managing directors must approve all request for access to employee's e-mail and computers, we found that different units in ISTS were following different practices. For example, according to an ISTS official, Help Desk requests to access employee e-mail and computers do not always go through managing directors. ISTS officials also acknowledged that there are no written procedures for contractors manning the ISTS Help Desk on how requests to access employee e-mail and computers should be handled. According to an agency attorney, without written procedures, GAO has little assurance that a consistent practice is followed on who is granted access and that only appropriate individuals receive access. In addition, while three units in ISTS handle access requests, ISTS does not (1) monitor these units' efforts, (2) document each request, and (3) have a database by which to track the total universe of requests. Further, while ISTS officials state that in a given year they receive few such access requests, without such a database, ISTS cannot really be assured of how many requests it has received and the nature of these requests.

We discussed with ISTS officials and GAO attorneys ways to strengthen the process by which supervisors and others access employee e-mail and computers. First, the officials and attorneys agreed that having a written policy would strengthen the overall control environment regarding such access. We discussed that such a policy should be disseminated to employees and should clearly state

- who can be granted access;
- what kind of information can be provided;
- when and how access can occur;
- the safeguards to prevent inappropriate access; and
- that employees have some expectation of privacy over personal information, such as doctor calendar appointments and medical information on their computers.

Having such a policy would constitute a best practice used in other federal agencies. For example, the Small Business Administration requires that agency officials must have written permission from the agency's chief information security officer and senior officials before monitoring employee e-mail.

Second, we discussed the need for written procedures for ISTS staff and contractors on how requests to access employee e-mail and computers are handled including how, when, and to whom access should be granted. Items discussed included that all requests should be in writing, be approved by the applicable unit head, and be maintained in the Help Desk tracking system. Having such procedures would support greater compliance with GAO Order 0510.2, Information Systems Security Policy, which requires (1) the implementation of policies and procedures to cost-effectively reduce risks to an acceptable level and (2) that all employee and contractor staff involved with GAO information systems be trained about their responsibilities for safeguarding GAO information and systems.

Third, we discussed that ISTS could modify the Help Desk tracking system to include requests from supervisors and others in order to oversee and monitor such access. We believe with such a modification that ISTS could better track and document these requests and maintain data by which to promote a more consistent approach on how access is granted.

Conclusion

Given the risks and internal control concerns regarding access to employee government e-mail and computers, we believe stronger controls over such access are needed. Having a written policy regarding access to employee e-mail and computers and written procedures for ISTS staff and contractors to follow when they receive such requests would strengthen the overall control environment regarding such access.

Recommendations

To strengthen the controls over access to employee government e-mail and computers, we recommend the Chief Administrative Officer

- Develop a written policy regarding supervisors and others access to employee e-mail and computers and inform employees of the policy. Such a policy should clearly state to whom, when, and how such access can occur; the safeguards present to prevent inappropriate access; and what personal information employees can have some expectation of privacy.

- Establish written procedures for ISTS staff and contractors handling requests to access employee e-mail and computers. Such procedures should require that all requests be in writing, be approved by the applicable unit head, and be maintained in the Help Desk tracking system.
- Expeditiously begin oversight and monitoring of requests to access employee e-mail and computers.

We discussed our review results and recommendations with the Chief Information Officer who generally agreed with our findings. The Chief Information Officer stated that GAO's General Counsel and the Managing Director of Knowledge Services would also be key players in developing and implementing actions in response to our recommendations.

Actions taken in response to our recommendations should be reported to my office within 60 days.