Office of Inspections and Forensic Auditing
Office of Inspector General
U.S. General Services Administration

Evaluation of 18F's Information Technology Security Compliance

JE17-002
February 21, 2017

Introduction

In December 2015, the Office of Inspector General (OIG) Office of Inspections and Forensic Auditing initiated an evaluation of the General Services Administration (GSA) Office of 18F, based on concerns expressed to us by several senior GSA officials about the management of 18F. Our report in that matter, *Evaluation of 18F* (Report No. JE17-001 (October 24, 2016)), described our findings of deficiencies in 18F's business operations.

During the course of that review, we also identified violations by 18F personnel of GSA information technology policies. On May 12, 2016, we issued *Management Alert Report: GSA Data Breach* (Report Number JE16-004). The report found that authorizations enabled by 18F staff while using Slack, an online messaging and collaboration application, potentially exposed sensitive information over the course of a five-month period. As a result of our alert report, GSA has since confirmed that content containing personally identifiable information (PII) was exposed to unauthorized users as a result of this breach.

We initiated this supplementary evaluation to take a broader look at whether 18F has complied with GSA's information technology security policies. This evaluation found that 18F routinely disregarded and circumvented fundamental security requirements related to both the acquisition of information technology and the operation of information systems.

Our report makes six recommendations to address the issues identified during the evaluation. In response to our report, GSA management agreed with our recommendations. Management's comments can be found in their entirety in the Appendix.

Background

18F, an office within GSA's new Technology Transformation Service (TTS), employs technology specialists who work with federal agencies to build, buy, and share digital services. A discussion of the formation and operations of 18F is contained in our *Evaluation of 18F*. As further background for this report, we briefly outline below relevant law and GSA policy addressing information technology security and acquisitions.

Chief Information Officers

The Clinger-Cohen Act of 1996 established Chief Information Officers (CIO) in federal executive agencies. The Act assigned the CIOs responsibility for appropriately acquiring and managing information technology, implementing a sound and integrated information technology architecture, and promoting the effective and efficient use of information resources.[1]

The Federal Information Security Management Act (FISMA) assigned additional responsibilities to CIOs. FISMA requires federal agencies, acting through their CIOs, to implement a

comprehensive framework for ensuring the development, maintenance, and effectiveness of information security controls over federal information and information systems.[2] FISMA requires information security protections to be commensurate with the risk and magnitude of the harm resulting from unauthorized use of agency information systems.

The Federal Information Technology Acquisition Reform Act (FITARA) further enhanced the CIO's role for information technology and information technology services by requiring CIOs to have a significant role in the management, governance, and oversight processes related to information technology, including oversight of information technology acquisitions.[3] While FITARA was not fully implemented at GSA at the time of our review, the terms of a June 2, 2015 Memorandum of Agreement (MOA) signed by 18F and GSA officials incorporated the FITARA requirement that the GSA CIO review and approve all agency information technology acquisitions.

GSA Information Technology Standards Profile

The Office of GSA IT (GSA IT) is responsible for ensuring that the agency's information technology security policies, procedures, and practices are adequate and in compliance with federal law.[4] In furtherance of this responsibility, GSA IT developed a portfolio of policies and procedural guidance to secure GSA information and information systems, including the GSA Enterprise Architecture Policy.[5]

As a foundation for the GSA Enterprise Architecture program, GSA IT implemented an Information Technology Standards Profile, which includes a list of software and cloud services approved for use in GSA's information technology environment.[6] The GSA Enterprise Architecture & Planning team within GSA IT determines and maintains GSA's Information Technology Standards Profile through a review process for all new information technologies. The review process includes a security review, a legal review, and a review for compliance with accessibility requirements.

All GSA staff share responsibility for adherence to and proper implementation of GSA IT security policy requirements.

Authorizations to Operate Information Systems

GSA information systems must be approved through the GSA security assessment and authorization process prior to operating in the GSA information technology environment.[7] The owner of the information system must work with GSA IT's Office of the Chief Information Security Officer to plan and test the security of the information system, and must submit a system security plan for that office to review. In order for an information system to be authorized to operate, the Chief Information Security Officer must concur with the review and sign an authorization to operate (ATO) letter that is then provided to the system authorizing official. The authorizing official may then grant authorization for the information system to operate.[8]

ATO letters specify an authorization period. Upon expiration of the period and in order to keep operating, information systems must be re-authorized with the concurrence of the Chief

Information Security Officer. Generally, information systems that hold more sensitive information (such as PII) will require an elevated level of scrutiny in the security assessment and authorization process.

Findings

18F disregarded fundamental GSA information technology security requirements and circumvented the CIO

GSA's internal information technology security policies identify fundamental requirements to obtain management authorization for information systems to operate. These policies also identify, among other things, requirements for the acquisition of information technology and acceptable use of email. We found that 18F disregarded GSA IT security policies for operating and obtaining information technology, and for using non-official email. 18F also created and used its own set of guidelines for assessing and authorizing information systems that circumvented GSA IT. We describe these compliance failures in detail below.

18F used information technology that was not approved by GSA IT

GSA offices acquiring or using information technology to conduct GSA business are required to ensure adherence to the Information Technology Standards Profile. In order to be included on the Information Technology Standards Profile, proposed new information technologies must undergo a formal review conducted by GSA IT to ensure the proposed information technology meets GSA's security, legal, and accessibility requirements.[9]

According to the GSA IT Chief Enterprise Architect, the Information Technology Standards Profile was created to ensure the security of the data of the organization and the network; to ensure that end user and terms of service agreements are reviewed by GSA's Office of General Counsel and found to be legally acceptable; to ensure accessibility, that software should be available to all; and to avoid redundancy so as to not waste resources.

We reviewed inventory lists of software in use by 18F and compared them to the Information Technology Standards Profile as of July 26, 2016. We found that 100 of the 116 software items listed, or 86 percent, had not been submitted for review and approval by GSA IT for use in the GSA information technology environment.

Examples of software that were in use by 18F, but not approved by GSA IT, included Hackpad, used for taking collaborative notes and sharing data and files; CloudApp, a visual communication platform; Pingdom, a website monitoring tool; and Hootsuite, a social media marketing and management dashboard. During our review, GSA IT determined that these software products should not be used in the GSA information technology environment and issued a notice to GSA staff in June 2016 that access to these and other software products would be blocked.

We interviewed the 18F Director of Infrastructure, whose responsibilities include ensuring compliance with information technology security policies and providing technical advice and direction to 18F. He told us that 18F is "definitely not compliant" with the Information Technology Standards Profile. He also told us that he was not aware of the profile until the OIG brought it to his attention in May 2016.

18F failed to obtain proper authorizations to operate information systems

The Office of the Chief Information Security Officer is responsible for reviewing and providing assurance that GSA information systems adhere to required federal and GSA IT security policies and procedures. Information systems can be of varying types, such as transaction processing and database management systems, and are used to perform functions such as complex calculations, automating workflows, searches, and analysis and review.[10] Examples of information systems used at GSA include human resources and inventory reporting systems.

Information systems are vulnerable to cybersecurity threats such as hacks, viruses, and malicious spyware. In order to mitigate threat vulnerabilities, the GSA Information Technology Security Policy requires that all information systems complete the security assessment and authorization process and receive an authorization to operate in the GSA information technology environment.[11] The Information Technology Security Policy also assigns specific security roles and responsibilities to ensure the effective implementation and management of GSA's information technology security program. As described above, the process requires the GSA Chief Information Security Officer's concurrence with the authorization.

We reviewed documentation for 18 information systems operated by 18F during the period June 1, 2015 to July 15, 2016, and found that none of the systems had proper authorizations to operate in the GSA information technology environment for the full period of our review. Two of the information systems had been in operation for six months or longer before they were authorized with concurrence by the Chief Information Security Officer. Five of the information systems had been properly authorized but continued to operate after their authorizations had expired. Eleven information systems were in operation without the Chief Information Security Officer's concurrence with their authorizations. When asked if the authorizations for these systems had been submitted for concurrence, the 18F Director of Infrastructure stated that they had not.

At least two of the 18F information systems that were operated without the required concurrence contained PII. In one such instance, 18F staff members integrated the online messaging and collaboration application Slack with their individual GSA Google Drives in October 2015. The vulnerability caused by the inappropriate integration was not discovered until March 2016, five months later. This incident was the subject of our May 12, 2016, Management Alert Report.

In response to our alert report, the 18F Executive Director and Director of Infrastructure co-authored a public blog post on May 13, 2016, stating, "We did a full investigation and to our knowledge no sensitive information was shared inappropriately."[12] 18F also subsequently issued emails to external partner agencies stating that "this was not a hack or data breach in any way, and this misconfiguration did not cause any sensitive information to be shared inappropriately." However, after concluding a comprehensive review of the incident in August 2016, GSA IT

found that the vulnerability exposed content containing PII to unauthorized users. As of February 2, 2017, the 18F blog post had not been updated to reflect the results of GSA IT's review.

Another instance of an 18F system holding PII that was operated without the required concurrence is a recruitment and applicant tracking information system containing applicants' résumés and contact information. In addition to operating this system without concurrence from the Chief Information Security Officer, 18F inappropriately categorized the level of risk for this system at a level below what the National Institute of Standards and Technology generally requires for information systems that hold PII. The GSA IT Director of Security Engineering told the OIG that he was not aware of 18F's use of this system until we brought it to his attention, and that 18F should have followed the established assessment and authorization process. By failing to obtain the required concurrence, 18F avoided the oversight of the Chief Information Security Officer and improperly understated the level of risk for the system.

18F circumvented the GSA IT assessment and authorization process

In addition, we found that 18F had circumvented GSA IT by creating and using 18F's own security assessment and authorization process.

In February 2015, the then Deputy Executive Director of 18F, Aaron Snow, proposed to then CIO Sonny Hashmi a new set of authorization guidelines, entitled "Guidelines for Granting Authority to Operate 18F-Hosted Open Data Systems." If these proposed guidelines had been approved by the CIO, they would have allowed 18F to authorize "low risk, open data" (*i.e.*, public) information systems meeting certain criteria without conducting the full security assessment and authorization process normally required. The proposal stated that "conducting a full security assessment of such systems before they are deployed would . . . be unnecessary and wasteful." GSA emails reflect that both CIO Hashmi and the Chief Information Security Officer expressed security concerns with 18F's proposal.[13]

We found that GSA IT did not approve the guidelines. However, 18F began using these guidelines to authorize information systems in February 2015. The Director of Infrastructure told us he received approval of the guidelines from Phaedra Chrousos, who at the time had oversight of 18F in her position as head of GSA's Office of Citizen Services and Innovative Technologies (OCSIT).[14] Chrousos told us that she remembered the Director's request for her signed approval of the guidelines shortly after she became head of OCSIT in early 2015. She said she did not recall signing them, but probably would have done so. At our request, TTS officials searched for any record of the guidelines and told us that they could not verify the existence of the signed document.

In addition, we found that 18F implemented a 'pre-authorization' policy under which other information systems 18F deemed low risk were authorized to operate without completing any security assessment and authorization process. The policy applied to information systems that met certain conditions, including systems that were deployed to the 18F cloud services environment, did not collect or store PII, and were available only to GSA staff or other federal agencies. 18F's timekeeping system, Tock, was one information system that was pre-authorized

using this process. The Chief Information Security Officer told us that 18F's pre-authorization policy was not permitted.

We also found that the 18F Director of Infrastructure appointed himself as the 18F Information Systems Security Officer (ISSO) when he became dissatisfied with the ISSOs GSA IT assigned to 18F. According to GSA policy, the Chief Information Security Officer is responsible for appointing ISSOs, who are responsible, among other things, for implementing and enforcing GSA's Information Technology Security Policy. The Chief Information Security Officer told us that he was not aware the 18F Director of Infrastructure had appointed himself as ISSO for 18F. He said that the Director should not have taken things into his own hands and his decision to go around the Chief Information Security Officer by naming himself the Information Systems Security Officer was not valid.

The GSA IT Director of Security Engineering told us that 18F has highly skilled developers who are confident that they write code and develop products without any security vulnerabilities; however, developers can still write bad code and that is why processes like the GSA IT ATO process are important. The use of information systems without the Chief Information Security Officer's knowledge and authorization limits GSA's ability to comply with FISMA requirements and risks the unauthorized access, use, disclosure, disruption, modification, or destruction of GSA information systems and information.

18F acquired information technology without the required Chief Information Officer review and approval

We also found that during the period of June 2, 2015 through July 15 2016, 18F entered into contracts and other agreements for the acquisition of information technology valued at over $24.8 million without obtaining review and approval of the contracts by GSA's CIO. These contracts included $21.5 million for infrastructure services, $2.5 million for support services, $484,641 for software, and $332,909 for hardware.

18F is required to obtain CIO approval for all acquisitions of information technology by the terms of a June 2, 2015 Memorandum of Agreement (MOA) that established 18F's funding source for operations. Incorporating FITARA's requirement that agency CIOs must have a significant role in the acquisition and oversight of information technology, the MOA stated:

> In accordance with the Federal Information Technology Acquisition Reform Act (FITARA), CIOs shall have a significant role in the decision processes for all annual and multi-year planning, programming, budgeting, and execution decisions, and the management, governance, and oversight processes related to information technology. GSA may not enter into a contract or other agreement to acquire information technology (IT) or IT services for internal purposes, unless the contract or other agreement has been reviewed and approved by the Chief Information Officer of GSA….

The 18F Director of Operations told us that he is the approver for the acquisition of information technology and services for 18F, and that prior to the OIG's Management Alert Report, the CIO did not review 18F's information technology purchases.

CIO Shive told us that he only reviewed contracts sent to him and would not have been aware of any 18F information technology acquisitions that were not sent to him for review. However, he acknowledged that he should have reviewed and approved 18F's acquisition of information technology in order to comply with the terms of the MOA.

18F staff used unofficial email accounts to conduct GSA business

Employees of an executive agency are prohibited from sending work-related emails using an unofficial email account unless the employee copies their official account when the message is first created or within 20 days after the original creation or transmission. GSA's Information Technology Security Policy reinforces this requirement.[15]

During the course of our review, we found that 27 unofficial email accounts belonging to 18F staff had been used to send work-related emails without copying or forwarding the messages to the employees' official GSA email account as required. Among the 27 unofficial email accounts used to conduct GSA business were those of the former TTS Commissioner, Phaedra Chrousos, a senior 18F advisor, and an 18F director. The work-related emails sent from these 27 accounts included information such as ongoing project details, a draft letter to Congressional legislators, 18F involvement with upcoming speaking events and conferences, account login information, documents related to official travel, issues with payments to an 18F vendor, and employee separations.[16]

The Federal Records Act also requires that agencies preserve official records, which include all work-related emails.[17] The National Archives and Records Administration issues regulations that dictate how records should be maintained. These regulations state that records must be maintained by the agency, be "readily found when needed," and that the records must "make possible a proper scrutiny by the Congress."[18] 18F's failure to maintain federal records in compliance with these laws and regulations puts at risk GSA's ability to document official business and limits the accessibility of these records to stakeholders.

18F and GSA IT Leadership failed to ensure compliance

We sought to determine the cause of 18F's widespread violations of fundamental GSA information technology security requirements. We concluded that management failures in GSA IT and 18F caused the breakdown in compliance.

We interviewed Andrew McMahon, GSA's Regional Administrator for Region 9 and Senior Technology Advisor, who has served as advisor to GSA's Administrator regarding 18F since its inception. McMahon told us that 18F was not permitted any flexibility regarding compliance with GSA information technology policies. He also told us that former CIO Hashmi was very involved with 18F from the beginning, particularly in a joint effort to improve the ATO process and in signing ATOs for 18F. 18F Executive Director Snow provided similar recollections of CIO Hashmi's involvement with 18F. We observed that, early on, 18F personnel demonstrated awareness of policy requirements by obtaining proper authorizations for several information systems.

With few exceptions, all 18F personnel completed GSA's mandatory online IT Security Awareness and Privacy 101 Training. The introductory paragraph in that training specifically referred and provided a link to the IT Security Policy. Moreover, 18F's Director of Infrastructure received a copy of the IT Security Policy in July 2014 directly from a GSA IT ISSO, who identified it to the Director as "pretty much the GSA IT Bible." This policy describes the roles of personnel responsible for information technology systems and information.

However, we found that senior leaders in 18F and OCSIT failed to ensure continued compliance with GSA IT security policies. Former OCSIT head Chrousos told us that 18F was not sufficiently integrated into the GSA IT environment. When asked about the compliance breakdown, she said that 18F technologists from the private sector do not "understand the same rules" regarding the security policies as GSA IT staff. When pressed regarding why she would have authorized an ATO process for 18F without GSA IT concurrence, Chrousos said that no one from GSA IT ever raised the question with her. She also apologized and said that she is not an IT engineer and therefore left technical matters to the Director of Infrastructure.

When we asked 18F Executive Director Snow why there was a breakdown in 18F's information technology security policy compliance, he answered, "I honestly don't know." According to Snow, 18F leadership was "hands-off" and there was not a lot of concern about compliance with GSA IT's information technology security policies at the time 18F was launched in March 2014. Snow also acknowledged that he had not ensured that GSA IT policies were being followed when he assumed leadership of 18F in May 2015. Neither Chrousos nor Snow told of any efforts on their part to engage GSA IT in order for their executive teams to gain a firm understanding of how GSA IT policies affect 18F operations.

The 18F Director of Infrastructure told us his team created an infrastructure to meet requirements of federal laws, but did not include GSA IT security policies in that framework. As noted, although the Director told us he had no training on GSA IT policies, we found that he completed the mandatory training, received a copy of the IT Security Policy from GSA IT, and had frequent discussions with the Chief Information Security Officer. We found that Chrousos and Snow failed to provide adequate oversight and guidance to subordinates, particularly to the 18F Director of Infrastructure, who was responsible for security, compliance with GSA IT policies, and for providing technical advice and direction. Ultimately, Chrousos' and Snow's indifference to GSA IT policies contributed to the compliance breakdown.

We found that the CIO also failed to ensure 18F's compliance with GSA IT security policy. When asked about the compliance failures, CIO Shive told us that before the OIG's Management Alert Report, he was "not in a position" to see what 18F was doing. He asserted that this was not because 18F was being secretive, but that 18F was operating as a separate unit with a start-up mentality. He also said that he did not want to scare people away by being "draconian," but wanted to spend time learning how they operate and strengthen the overall relationship. However, the CIO is responsible for the GSA information technology security program, and has been granted broad authority for that purpose. He must provide guidance, assistance, and management processes to enable GSA entities and staff to comply with security policy. The CIO must also provide oversight and verify compliance with GSA IT policies. The CIO failed to fulfill these responsibilities.

Conclusion

We found that management failures in GSA IT and 18F caused a breakdown in compliance with GSA information technology security requirements. Leadership failed to provide sufficient guidance and oversight to ensure the proper level of awareness and compliance. As a result, 18F routinely disregarded and circumvented fundamental GSA information security policies and guidelines.

Recommendations

1. TTS and GSA IT should identify all 18F information systems and ensure they are authorized to operate in accordance with the GSA's Information Technology Security Policy (CIO 2100.1J).

2. TTS and GSA IT should ensure all information technology used by 18F is in compliance with, and approved by, GSA IT.

3. TTS should ensure that 18F staff uses only official email accounts to conduct GSA business.

4. TTS should ensure that all federal records sent from unofficial email accounts are copied into official GSA email accounts as required by the GSA Information Technology Security Policy.

5. TTS should ensure compliance with FITARA and the terms of the June 2, 2015 Memorandum of Agreement that requires CIO review and approval of all contracts or other agreements entered into by 18F to acquire information technology or information technology services.

6. GSA IT should develop training for GSA senior level leaders regarding information technology security roles and responsibilities.

Objectives, Scope, and Methodology

This evaluation was conducted by the Office of Inspections and Forensic Auditing to determine whether 18F complied with GSA's information technology security policies. In order to accomplish our objectives, we:

- Researched laws, rules, regulations, and other federal guidance that establish the legal and operational requirements for managing federal information systems and information technology resources;
- Reviewed GSA policies, orders, and procedures related to the management of information systems and information technology resources;
- Reviewed GSA IT guidance and oversight related to the acquisition and use of information technologies;
- Reviewed relevant audits and inspections conducted by GSA OIG, GAO, and other federal agencies;
- Interviewed agency management and staff from GSA IT and 18F;
- Analyzed contracts and agreements entered into for 18F to acquire information technology and information technology services;
- Analyzed inventory lists of software and information systems in use by 18F;
- Reviewed security assessment and authorization documentation issued for information systems operated by 18F;
- Reviewed security incident reports filed by 18F with the Office of the Chief Information Security Officer;
- Reviewed records of scans and audits of 18F information technology systems conducted by GSA IT;
- Reviewed training records for 18F staff; and
- Reviewed email documentation for 18F staff.

Our evaluation was conducted from April 2016 through December 2016 in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation* (January 2012).

Endnotes

[1] Pub. L. No. 104-106, § 5125(b) (1996), *currently codified at* 40 U.S.C. § 11315. All Westlaw United States Code citations are current through Pub. L. 114-316 (including Pub. L. No. 114-318 to 114-321, 114-323 to 114-327, and 115-1 to 115-3).

[2] Pub. L. No. 107-347, § 301 (2002), *currently codified at* 44 U.S.C. § 3554.

[3] Pub. L. No. 113-291, § 831 (2014), *currently codified at* 40 U.S.C. § 11319.

[4] GSA Order ADM O 5440.667, *Change in GSA Office of the Chief Information Officer and Office of Citizen Services and Innovative Technologies* (August 5, 2014), renamed the Office of the Chief Information Officer (OCIO) as the Office of GSA IT.

[5] GSA Orders CIO 2110.2, *CIO GSA Enterprise Architecture Policy* (November 26, 2008), and CIO 2110.3, *CIO GSA Enterprise Architecture Policy* (September 29, 2015).

[6] GSA Orders CIO P 2160.1E, *General Services Administration (GSA) Information Technology (IT) Standards Profile* (February 12, 2014), and CIO 2160.1F, *General Services Administration (GSA) Information Technology (IT) Standards Profile* (September 9, 2016).

[7] GSA Orders CIO P 2100.1I CHGE 1, *GSA Information Technology (IT) Security Policy*, (October 20, 2014) at Ch. 3, CIO P 2100.1J, *GSA Information Technology (IT) Security Policy* (December 22, 2015) at Ch. 3, and CIO P 2100.1J CHGE 1, *GSA Information Technology (IT) Security Policy*, (April 28, 2016) at Ch. 3.

[8] The security assessment and authorization process is based upon and derived from the Risk Management Framework found in NIST SP 800-37 for the assessment, authorization, and operation of information systems.

[9] GSA Orders CIO P 2160.1E, *General Services Administration (GSA) Information Technology (IT) Standards Profile* (February 12, 2014), at (5)(a) and CIO 2160.1F, *General Services Administration (GSA) Information Technology (IT) Standards Profile* (September 9, 2016), at (5)(a). GSA Order CIO 2160.1F also requires approval by the Chief Technology Officer.

[10] The GSA Information Technology Security Policy refers to the definition of information system found in OMB Circular A-130, which reads, “The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.”

[11] GSA Orders CIO P 2100.1I CHGE 1, *GSA Information Technology (IT) Security Policy* (October 20, 2014) at Ch. 3, CIO P 2100.1J, *GSA Information Technology (IT) Security Policy* (December 22, 2015) at Ch. 3, and CIO P 2100.1J CHGE 1, *GSA Information Technology (IT) Security Policy* (April 28, 2016) at Ch. 3.

[12] Aaron Snow and Noah Kunin, “How 18F Handles information security and third party applications,” May 13, 2016, <https://18f.gsa.gov/2016/05/13/how-18f-handles-information-security-and-third-party-applications/> accessed on February 2, 2016.

[13] The Chief Information Security Officer was previously known as the Senior Agency Information Security Officer under GSA Order CIO P 2100.1I CHGE 1, *GSA Information Technology (IT) Security Policy* (October 20, 2014), but was revised under GSA Order CIO 2100.1J, *GSA Information Technology (IT) Security Policy* (December 22, 2015).

[14] Phaedra Chrousos served as the Associate Administrator for GSA's Office of Citizen Services and Innovative Technologies from January 2015 to May 2016, and as the Commissioner of the Technology Transformation Service from May 2016 to July 2016.

[15] GSA Orders CIO P 2100.1J, *GSA Information Technology (IT) Security Policy* (December 22, 2015) at Ch. 4, (2)(p)(7), and CIO P 2100.1J CHGE 1, *GSA Information Technology (IT) Security Policy*, (April 28, 2016) at Ch. 4, (2)(p)(7).

[16] Due to the large volume of emails that we collected, we limited our review to determining how many unofficial email accounts violated GSA policy but not the full extent to which each unofficial email account violated the policy.

[17] Pub. L. No. 81-754 (1950), *currently codified as amended at* 44 U.S.C. §§ 3101, 3301.

[18] 36 C.F.R. §§ 1222.34, 1222.22(c) (Westlaw through Feb. 9, 2017).

Appendix: Management Comments

GSA

Technology Transformation Service

February 16, 2017

MEMORANDUM FOR PATRICIA D. SHEEHAN
Assistant Inspector General for Inspections
Office of Inspector General

FROM: Robert L. Cook
Commissioner, Technology Transformation Service (TTS)
US General Services Administration (GSA)

SUBJECT: Draft Report *JEF16-005-002 Evaluation of 18F's Information Technology Security Compliance*

Thank you for the Office of Inspector General's (OIG) draft report entitled *Evaluation of 18F's Information Technology Security Compliance* (JEF-16-005-002), dated February 2, 2017, and conducted from April to December, 2016. I appreciate the review of TTS's compliance with GSA's information technology (IT) security practices. In addition to being one of the top priorities for GSA, IT security is a top priority of TTS and our systems-focused offices, especially 18F.

GSA understands that there were notable gaps in compliance with GSA IT security requirements, and agrees with OIG's recommendations. We appreciate the May 12, 2016, OIG Management Alert Report, received mid-way through the audit, as it enabled GSA to immediately initiate work on corrective actions.

Working in partnership, TTS and GSA IT have implemented significant changes to ensure compliance with GSA IT security requirements. The GSA Chief Information Officer (CIO) has directed and I have assured him that he will have full visibility into 18F's IT activities. This includes Chief Information Security Officer review and approval of authorizations for system operation, GSA IT approval of TTS software use approved through GSA IT's standards process, and CIO review and approval of IT contracts and agreements as required by the Federal Information Technology Acquisition Reform Act.

TTS and GSA IT worked together to identify all unapproved software in use and created a process that was used to either approve or cease use of such applications or systems. TTS and GSA IT now ensure new software requests go through the revised GSA IT standards process for review, which allows for better communication about needs and priorities. TTS and GSA IT also established a process by which the GSA CIO receives covered TTS contracts and agreements for review and approval.

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

GSA

Technology Transformation Service

TTS takes seriously its partnerships with and responsibility to other federal agencies and the public. As an IT service and solution partner, TTS works diligently to preserve the integrity of government systems while being innovative in a constantly changing environment. TTS is committed to rigorous security and compliance practices. As an example, TTS was recently granted a Provisional Authority to Operate TTS's cloud.gov by the FedRAMP Joint Authorization Board.

As TTS works to ensure the rigor of its IT security compliance, we look forward to OIG oversight and input, and the opportunity to prepare action plans responding to the OIG recommendations. If you have any questions, please contact Ms. Amber Van Amburg at 202-603-8011 or amber.vanamburg@gsa.gov.

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

OFFICE OF INSPECTOR GENERAL

U.S. General Services Administration

For media inquiries

OIG_PublicAffairs@gsaig.gov

(202) 273-7320

(800) 424-5210

Anonymous Web Form

fraudnet@gsaig.gov

Want to be aware of information the instant it becomes publicly available?

SUBSCRIBE

REPORT FRAUD, WASTE, AND ABUSE!