Audit Report

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

August 7, 2009

Office of Inspector General
General Services Administration

Office of Audits

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

August 7, 2009

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: August 7, 2009

Reply to Attn of: Deputy Assistant Inspector General for Auditing
Information Technology Audit Office (JA-T)

To: Kathleen M. Turco
Chief Financial Officer, Office of the Chief Financial Officer (B)

Subject: FY 2009 Office of Inspector General Information Technology Security Audit of the E2 Travel System Security Controls
Report Number A080180/B/T/F09008

This audit report presents the results of our review of select management, operational, and technical security controls for the General Services Administration's (GSA) implementation of the E2 Travel System. E2 is a government-wide, web-based service intended to provide travel management practices to consolidate Federal travel, minimize cost, and produce superior customer satisfaction. While the GSA Office of the Chief Financial Officer (OCFO), with the assistance from the Federal Acquisition Service (FAS) Program Management Office (PMO), has applied the majority of the security measures required by GSA's Information Technology (IT) Security Program with the Agency's implementation of E2, we identified specific security controls that require management attention in order to ensure that GSA's sensitive financial and travel information is adequately safeguarded and that the confidentiality, integrity, and availability of the E2 system is maintained within the Agency's operational environment. As discussed, Appendices D through F that include sensitive system security information will be restricted to system security officials and the GSA Senior Agency Information Security Officer.

Certification and accreditation (C&A) and risk management processes can be improved by addressing not only the government-wide solution but also risks and vulnerabilities specific to GSA's IT systems environment. This would better enable GSA to mitigate threats that could lead to system exploits and to protect sensitive information. We also found the opportunity to improve GSA's ability to effectively prevent, detect, and recover from an attack by ensuring that agreements have been developed for each interconnection with E2. Contractor oversight can also be improved by ensuring that required personnel background investigations are completed and security awareness training is taken prior to providing contractors with full system access. Further, actions should be taken to strengthen system security by implementing two-factor authentication for user access to E2 and by restricting access to privileged procedures and user training materials to those with a need-to-know. Additional improvements can also be made to strengthen system security by assessing whether use of secure e-mail addresses for resetting user account passwords and whether use of an official approved web domain for accessing the system is needed. Finally, strengthening configuration management processes for E2 by addressing identified technical weaknesses with system databases and device configurations would provide extra protection for the system and its sensitive information. Written comments that you provided to the draft report are included as Appendix G.

I wish to express my appreciation to you, your staff, staff from the Federal Acquisition Service (FAS) Program Management Office (PMO), and individuals with system security responsibilities for their assistance with this audit. If you have any questions regarding our review of security controls for GSA's implementation of E2, please contact me or Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits, on 703-308-1223.

Jennifer M. Klimes
Audit Manager
Information Technology Audit Office (JA-T)

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

TABLE OF CONTENTS

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

EXECUTIVE SUMMARY

Purpose

In December 2006, the General Services Administration (GSA) implemented E2 Solutions (E2), an operational system that is maintained for agencies by a Federal contractor, to provide for its travel management needs. The system currently processes approximately 36,000 temporary duty and local travel vouchers per year covering $28.2 million in travel expenses for GSA travelers. E2 is a moderate risk[1] Privacy Act System of Record[2] that contains personally identifiable information (PII) as well as financial and travel data. The E2 system is included in GSA's Federal Information Security Management Act of 2002 (FISMA) inventory maintained by the GSA-Chief Information Officer (CIO), and will be included in our Fiscal Year (FY) 2009 FISMA report The objective of this information security review of E2 was to determine if GSA has implemented management, operational, and technical security controls to effectively manage risks inherent with a travel and financial management system which holds PII in accordance with FISMA and the Agency's Information Technology (IT) Security Program. If not, what additional actions are needed to better manage IT security risks for the system? Appendix A provides our objective, scope, and methodology for the audit.

Background

Expanding Electronic Government (e-Gov) is one of the key elements of the President's Management Agenda (PMA) initiated by President George W. Bush in July 2001. The e-Gov initiative goals include more results-oriented, efficient, and citizen-centered processes for the Federal government. GSA is the managing partner for the e-Gov Travel Service (ETS) initiative, one of the 24 initiatives included in the PMA. The ETS was launched in April 2002 to meet the goals of the PMA. It is a Government-wide, web-based service intended to provide travel management practices to consolidate Federal travel, minimize cost, and produce superior customer satisfaction. Goals for ETS include developing a Government-wide, web based, world-class travel management service; establishing a cost model that reduces or eliminates capital investment and minimizes total cost per transaction for the government; and creating a policy environment based on the use of best travel management policies.

[1] Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, requires Federal agencies to classify their information systems into one of three risk levels: low, moderate, or high. GSA's designation of E2 as moderate risk means that the Agency has made a determination that the loss of system confidentiality, integrity, or availability could be expected to have a serious effect on organizational operations, organizational assets, or individuals.

[2] A Privacy Act System of Record is a system containing information that is retrieved by an individual's name or other unique identifier assigned to the individual. This information is protected under the Privacy Act of 1974.

In November 2003, the GSA Federal Acquisition Service (FAS) Program Management Office (PMO) awarded three competitively bid contracts to vendors to implement the ETS and provide for web-based, travel management services for the Federal government until 2013. The master contract with Carlson Wagonlit Government Travel (CWGT) was for use of its E2 Solutions (E2), one of the three systems offered under the ETS initiative. Under this contract, the GSA Chief Financial Officer (CFO) selected E2 to provide for travel management services for GSA Associates. The FAS-PMO subsequently issued a task order to CWGT in January 2005 to implement E2 within GSA.

The FAS-PMO is responsible for ensuring FISMA requirements, including policies and procedures established with the GSA IT Security Program, have been implemented for the Government-wide E2 system. Within GSA, the OCFO is responsible for ensuring the implementation of adequate security controls for its specific implementation of E2. CWGT is responsible for providing adequate physical security for both the major application (E2 Solutions) and the general support system that hosts it and for providing disaster recovery services. A diagram of roles and responsibilities related to the security portion of GSA's implementation of E2 is provided in Appendix B.

Results in Brief

The GSA-OCFO, with assistance from the FAS-PMO, has applied many of the security measures required by GSA's IT Security Program with the Agency's implementation of the E2 system. Our testing for 99 of 171 required baseline security controls found no reportable conditions for 88 controls. However, specific management, operational, and technical controls required with FISMA should be strengthened to ensure that sensitive financial and travel information is adequately safeguarded and the confidentiality, integrity, and availability of the E2 system is maintained. Opportunities exist to strengthen certification and accreditation (C&A) and risk management processes by addressing not only the Government-wide solution but also risks and vulnerabilities specific to GSA's IT systems environment. This would better enable GSA to mitigate threats that could lead to system exploits and to protect sensitive information. We also found the opportunity to improve GSA's ability to effectively prevent, detect, and recover from an attack by ensuring that agreements have been developed for each interconnection with E2. Contractor oversight can also be improved by ensuring that required personnel background investigations are completed and security awareness training is taken prior to providing contractors with full system access. Further, actions should be taken to strengthen system security by implementing two-factor authentication for user access to E2 and by restricting access to privileged procedures and user training materials to those with a need-to-know. Additional improvements can also be made to strengthen system security by assessing whether use of secure e-mail addresses for resetting user account passwords and whether use of an official approved web domain for accessing the system is needed. Opportunities also exist to strengthen configuration management processes for E2 by addressing identified technical weaknesses with system databases and device configurations. This would provide extra protection for the system and its sensitive information.

Recommendations

To better manage IT security risks with the GSA implementation of E2 and ensure the confidentiality, integrity and availability of this system and the data it maintains, we recommend that the Office of the Chief Financial Officer (OCFO) work with the Federal Acquisition Service (FAS) Program Management Office (PMO) and the Office of the Chief Information Officer (OCIO), to take actions to strengthen:

1. Management controls by:

a) Ensuring that controls for and risks with GSA's implementation of E2, specific to the GSA IT systems environment, have been adequately addressed.
b) Establishing a Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) for the E2 interconnection with the Global Distribution System (GDS).

2. Operational controls by:

a) Obtaining assurance that an adequate process is in place and being used to effectively track the completion of background investigations and annual security awareness training prior to providing contractors with full access to GSA data.

3. Technical controls by:

a) Identifying those users with privileged access and expedite implementation of two-factor authentication for those users.
b) Restricting access to privileged procedures to those with a need-to-know.
c) Ensuring that GSA-Chief Information Officer (CIO) hardening guides are applied.
d) Disabling unnecessary functionality to eliminate the threat posed by providing non-essential services and ensuring that software running on the networked servers is properly patched to their most recent versions.
e) Determining whether a *.com* domain is necessary for the proper performance of the operation of the E2 Solutions (E2) travel system, or whether an approved web domain, such as *.gov*, *.mil*, or *.Fed.us* should be used.
f) Developing IT Security procedures to restrict the transmission of sensitive information, including password resets, to government e-mail addresses.

Management Comments

Our recommendations are directed to the GSA-CFO and focus on specific improvements for management, operational, and technical controls needed to strengthen security for GSA's implementation of the e-Government Travel Services E2 Solutions system. The CFO generally agrees with our findings and recommendations, and a copy of the written management response to our draft report is provided in Appendix G. Included in the management comments are views from the FAS-PMO, who has responsibilities for ensuring that FISMA requirements are met for the government-wide E2 Solutions also offered by GSA to other Federal agencies. As discussed in our report, the GSA Office of the CFO is responsible for ensuring the implementation of

adequate security controls for the Agency's implementation of the e-Government Travel Services E2 Solutions system as GSA's official travel management solution. With this FISMA security audit, we also considered the key role of the GSA Senior Agency Information Security Officer who is responsible, within the GSA IT Security Program, for ensuring that systems that hold Federal data comply with all FISMA requirements and that controls for these systems are risk-based and within reasonable cost for the benefit provided. Our position, as noted throughout the report, is that GSA's IT Security Program should ensure that risks are being managed with GSA e-Government systems, including this e-Government Travel Services E2 Solutions system. While some issues raised may require specific actions from the FAS-PMO for the government-wide e-Travel solution, our audit did not include a focused assessment of government-wide security requirements for e-Government systems or full capabilities of the broader e-Government Travel Services E2 Solutions system offered by the FAS-PMO. Included in the CFO's comments to our draft report is a response from the FAS-PMO that indicates disagreement related to two of our recommendations to the GSA-CFO.

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

INTRODUCTION

The Federal Information Security Management Act of 2002 (FISMA) provides a framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and resources. It also includes for a mechanism to provide oversight of Federal agency information security programs. FISMA directs Inspectors General to perform an annual independent evaluation of their respective agency's information security program and controls for select systems. This report presents the results of our assessment of select management, operational, and technical security controls required by FISMA for the E2 Solutions (E2) system. Appendix A provides our objective, scope, and methodology for the audit.

E2 is a financial management Privacy Act System of Record[3] that is operated and maintained by Carlson Wagonlit Government Travel (CWGT). It is one of three systems that the General Services Administration (GSA) Federal Acquisition Service (FAS) Program Management Office (PMO) offers for e-Gov Travel Service (ETS) and is designated by the Agency as "moderate risk[4]." In January 2005, the GSA Office of the Chief Financial Officer (OCFO) selected E2 as the e-Travel system to provide travel services for the Agency. GSA implemented E2 in December 2006. GSA travelers can access E2 directly from the Internet, or from behind GSA's network firewall. E2 processes sensitive but unclassified information, including personally identifiable information (PII), financial data, credit card information, and transaction amounts. GSA introduced miscellaneous reimbursement capabilities through E2 that are not associated with official travel in October 2008. For GSA's implementation of E2, the OCFO is responsible for managing user accounts, including authorizing system access and approval routing, and for implementing appropriate Agency travel policy. The FAS is responsible for working with CWGT to make any approved system changes, for ensuring the contractor implements appropriate security controls, and for managing the master contact with the ETS vendors.

In January 2006, the GSA Office of the Inspector General (OIG) Information Technology (IT) Audit Office issued a letter report[5] that conveyed the results of our assessment of select information security controls for E2 during Fiscal Year (FY) 2005. At that time, we found that steps taken to implement GSA's IT Security Program and FISMA requirements for E2 were not always consistent with Agency policy and National Institute of Standards and Technology (NIST) guidance. Specifically, required security controls and rules of behavior for third party system interconnections had not been included in the system security plan or authorized as part of the system Certification and Accreditation (C&A), and the system Plan of Action and

[3] A Privacy Act System of Record is a system containing information that is retrieved by an individual's name or other unique identifier assigned to the individual. This information is protected under the Privacy Act of 1974.
[4] For more information on system risk levels, refer to FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
[5] FY 2005 Office of Inspector General Information Security Analysis of the Carlson Wagonlit eTravel System, Report Number A050183/O/T/F06005, January 19, 2006.

Milestones (POA&M) did not include all known security weaknesses identified in the risk assessment, security plan, and contingency plan test. We also reported that, while background checks had been initiated for CWGT contractors supporting the system, those checks were not always in line with GSA's IT Security Policy. Vulnerability scanning conducted during our previous audit also identified specific system security weaknesses that required actions to strengthen system security.

RESULTS OF AUDIT

The General Services Administration (GSA) Office of the Chief Financial Officer (OCFO), with the assistance of the Federal Acquisition Service (FAS) Program Management Office (PMO), has applied many of the management, operational, and technical controls required by the Federal Information Security Management Act of 2002 (FISMA) and the GSA Information Technology (IT) Security Program for the E2 Solutions (E2) system. We tested 99 of 171 required baseline security controls and found no reportable conditions for 88 controls. See Appendix C for a detailed listing of the security controls tested. We have identified improvements that are needed to enhance risk management practices and provide improved security for GSA's implementation of the E2 system.

Risk management practices for E2 can be improved by strengthening management controls required for and risks specific to GSA's implementation of the system. Management controls can also be improved by ensuring that all needed risk assessment components, including threat identification and threat likelihood levels, are assessed. This could ensure that potential threats are addressed and reduce the likelihood that the system is exploited. Establishing agreements for a group of external systems that interface with E2 would better assist GSA with defining responsibilities for and coordinating actions in the event of a security incident. We also found that improvements can be made to enhance operational controls for GSA's implementation of E2. For instance, contractors are being provided full system access prior to the successful completion of background investigations and security awareness training. Opportunities also exist to improve technical controls for GSA's implementation of E2, such as implementing two-factor authentication for user access to the E2 system to more securely authenticate users to better protect GSA travel information and restricting access to privileged information to those with a need-to-know. Additional technical control improvements can be made to strengthen system security, including assessing whether use of an approved web domain should be required for accessing E2 and whether use of a secure e-mail address for account password reset is needed. Configuration management vulnerabilities that could affect the confidentiality, integrity, and availability of GSA's data were also identified. Technical weaknesses with the system database and device configuration demonstrate the need to strengthen configuration management practices to provide additional protection for the system and its sensitive data, including applying critical patches to the E2 servers. Throughout our audit we have kept E2 system security officials informed of our security control test results, and system security officials have either taken or informed us that they plan to take actions to mitigate risks related to several vulnerabilities identified in our testing. For example, system security officials are taking actions to enhance the security posture of E2 by disabling non-essential web server functionality, applying appropriate patches, securing account log-in procedures, and planning to review its password policy. Given the importance of this system and the travel and financial information it maintains, the OCFO and FAS-PMO should take additional steps to strengthen management, operational, and technical controls, to better manage risks with this important system.

Management Controls

Management security controls consist of safeguards or countermeasures that focus on the management of risk and information system security and include certification[6] and accreditation[7] (C&A), risk assessment, security planning, and integrating security requirements into system and services acquisition processes. The OCFO and FAS-PMO have applied many of the management controls required with FISMA for E2 (see Appendix C). However, we found the need to strengthen specific controls to ensure that risks were being managed for GSA's implementation of E2. The certification and accreditation (C&A) completed for E2 was for the Government-wide solution offered to any Federal agency and did not include controls implemented for or risks with GSA's implementation of E2, specific to the GSA IT systems environment. By not assessing controls for specific risks with GSA's implementation of E2, threats may not be properly identified, prioritized, and mitigated, possibly leaving the Agency without necessary compensating controls in place to reduce the likelihood of system exploits. We also identified one instance where E2 did not have needed agreements to specify responsibilities and controls for establishing, operating, and securing a system interconnection. Specific controls should be identified and stipulated to help prevent, detect, and deter from potential system security breaches.

Certification and Accreditation Completed for E2 Did Not Consider Controls for and Risks with GSA's Specific IT Systems Environment

A C&A was completed for the CWGT Government-wide E2 system solution that considered the complete array of security controls that are available to any Federal agency. Under the ETS initiative, Federal agencies first select one of the three systems available and then decide which features to implement from the overall solution offered by the vendor. We found that GSA has not yet documented the specific controls for the Agency's implementation of E2, and therefore, has not considered unique threats for GSA's operational environment. While some steps have been undertaken to assess risks for GSA's implementation of E2, specific actions are needed to strengthen the security posture of the system and ensure that risks within GSA's IT systems environment are adequately prioritized and mitigated to better protect sensitive data and transactions.

FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. It also requires this to be done for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. GSA information systems are required to be certified and accredited in accordance with National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-53, NIST SP 800-37, and the GSA Information Technology (IT) Security Policy. An Authorizing Official (AO) is required to authorize, in writing, information systems before they go into operation, accept any

[6] Certification refers to the process utilized to determine the extent to which controls are implemented correctly and operating as intended.

[7] Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations, assets, or individuals based upon the implementation of controls.

identified and unmitigated risks, and identify any deviations from the GSA IT Security Policy. These unmitigated risks and deviations from the IT Security Policy are known as residual risks.

System security documentation for E2 included information on baseline security requirements and system categorization but did not address system boundaries or threat identification, which would identify all potential threats to the system. Additionally, an e-authentication risk assessment, which included risk tolerance criteria, a risk transaction summary, and risk analysis, was performed in September 2004. However, these risk management actions are not sufficient because vulnerabilities or risks specific to GSA's implementation of E2 have not been identified. Risks must be assessed with the certification and accreditation for GSA's systems to ensure that security controls addressing associated risks have been appropriately implemented. Unidentified threats can lead to system exploits, leaving GSA's data at risk.

GSA security guidance on mitigating risk describes the key activities in managing enterprise-level risk for GSA's IT systems to ensure controls are implemented correctly and operating as intended. By relying solely on the C&A conducted on the Government-wide solution, GSA has not identified any unmitigated risks or deviations from the Agency's IT Security Policy, such as not having implemented two-factor authentication and not having written management authorization for every system interconnection. A consolidated C&A has benefits, including reducing Federal agency resources to document and assess the effectiveness of security controls generic to the E2 Government-wide solution. However, it is important to ensure that the controls for and risks with E2, as implemented within GSA's IT systems environment, have been addressed to evaluate risks specific to GSA and determine an overall level of risk the Agency is willing to accept. Reconsidering specific residual risks with E2 operations could also guide GSA in implementing compensating controls that may be needed to protect Agency travel and financial data.

Additional Actions Are Needed to Establish Required System Interconnection Agreements

Interconnections[8] are used to provide E2 users with travel availability and pricing information. The system feeds financial data captured on travel transactions through an interconnection to the Agency financial System of Record, Pegasys. See Appendix D for a diagram of interconnections with E2. E2 relies on the Global Distribution System (GDS), multiple private companies providing specific pricing, scheduling, and transaction information for airlines, hotels, and other services. The GDS is a commercial system that processes sensitive information, including charge card account numbers and other PII. This review identified that an ISA/MOU has not been established for the interconnection with the GDS.

The GSA IT Security Policy requires written management authorization based on an acceptable level of risk before connecting an Agency IT system to other systems. This written authorization should define the rules of behavior and controls that must be maintained for the system interconnection. NIST recommends that information technology (IT) systems should develop an Interconnection Security Agreement (ISA) (or an equivalent document) to document the technical requirements of the interconnection. These agreements help to guide the planning,

[8] NIST defines system interconnection as the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

establishment, maintenance, and termination of system interconnections where sensitive data and transactions incur risks. An ISA specifies the technical and security requirements for establishing, operating, and securing an interconnection. An MOU defines the purpose, identifies relevant authorities, specifies responsibilities, and defines the terms of the agreement. The development of these documents represents a proactive approach to security, as system management is able to make plans for prevention, deterrence, and detection of attacks rather than delaying decisions or appropriate actions until after a breach of security.

Our January 2006 FISMA letter report on the CWGT E2 Solutions Government-wide system identified that an ISA/MOU was not in place for the E2 interconnection with the GDS. In response to that report, this finding was listed in the E2 system Plan of Action and Milestones (POA&M). While the updated POA&M reports that an ISA/MOU had been developed in June 2007, our current review found that the ISA/MOU was not yet in place for the E2/GDS interconnection. According to system management, these agreements were not developed because the GDS rely on commercial legacy systems that are used by travel agencies to make reservations for official and leisure travel. Without interconnection agreements in place for GDS systems, the rules for interconnecting systems and for protecting data shared between E2 and other feeder systems have not been identified. Consequently, it may be more challenging to prevent, deter, detect, and recover from an attack, as notification of the attack may be delayed and proper audit trails may not be captured and maintained, as necessary.

Operational Controls

Operational security controls address methods that are primarily implemented by people, as opposed to systems, and include measures such as contingency planning, maintenance, configuration management, awareness and training, incident response, media protection, physical and environmental protection, system and information integrity, and personnel security. While security officials have implemented many of the operational controls required with FISMA for E2 (see Appendix C), we identified opportunities to strengthen operational controls by ensuring that contractor background investigations are completed and security awareness training is provided to contractors prior to providing them with full system access.

Providing Contractors with Full System Access Prior to Successful Completion of Background Investigations Increases Risk to the System

GSA's IT Security Policy requires that background investigation requirements for access to GSA information systems, including contractor systems containing GSA information, should be completed in accordance with the GSA Handbook ADM 9732.1C, *Suitability and Personnel Security.* Additionally, contractors working on Federal systems need to have a National Agency Check with Credit Inquiries (NACIC) equivalent or higher background investigation and fingerprint checks completed prior to being granted full access to a system. While waiting on the background investigations, contractors can be given temporary access, limited to a need-to-know, after successful fingerprint checks have been received. The Project Manager and/or Information Systems Security Officer (ISSO) are responsible for identifying all contractors who need background investigations and for ensuring that they are successfully completed prior to providing contractor personnel with full system access. Our review of E2 found that there

currently is no confirmation of successful completion of fingerprint checks or proof of adjudication and that there is no process in place to ensure that background investigations were both requested and completed. Subsequently, contractors are being provided with full system access prior to having their background investigations completed.

According to system security officials, CWGT conducts employment history, education verification, and criminal background checks on employees during the hiring process; however, this does not satisfy GSA's requirements. Because CWGT contractors were provided full system access prior to the completion of required background investigations, the E2 System is operating at greater risk of an insider attack.

Improvements to Verify Security Awareness Training for Contractor Personnel Are Needed

Agencies are required to provide appropriate information system security training to personnel, including contractors and other users of information systems, prior to allowing them to perform their assigned duties. Agencies must also document and monitor individual information system security training activities, including basic security awareness training and role-based information system security training. This training is necessary to inform users of information security risks associated with their activities as well as their responsibilities in complying with Agency policies and procedures designed to reduce these risks. GSA's IT Security Policy also requires all GSA employees and contractors to complete security awareness and privacy training annually to ensure that GSA, other agency, and contractor support staff involved in the management, design, development, operation, and use of IT systems are aware of their responsibilities for safeguarding GSA systems and information. While CWGT has implemented a tracking system to record the details of security training provided to its employees, for the sample we tested, CWGT was unable to verify that security awareness training was completed for all contractor personnel with system access. Our analysis of contractor security awareness training records reflected that processes were not in place to ensure records were properly maintained to verify the status of security awareness training. This has left GSA without confidence that adequate training was completed by CWGT prior to providing its staff with system access. Completion of GSA's security awareness training is important to ensure that everyone with access to the system knows their responsibilities for complying with Agency policies and procedures and is aware of their responsibilities related to safeguarding the system and its sensitive data.

Technical Controls

Technical controls focus on security capabilities executed by computer systems and include access controls, audit and accountability, identification and authentication, and system and communications protection. While the configuration settings control is identified by NIST as an operational control, technical control weaknesses we identified were related to configuration management, so it is included in this section of the report. Many of the technical controls required with FISMA have been implemented for E2 (See Appendix C). However, we found that opportunities exist to improve technical controls by implementing two-factor authentication and restricting access to privilege procedures to those with a need-to-know. We also identified configuration weaknesses with the operating system and database, which left system components

vulnerable to attacks that could lead to unauthorized access and a compromise of the E2 system. Additionally, security can be strengthened by determining whether use of an approved web domain should be required to access E2 and whether use of a secure e-mail account should be required to reset user passwords.

Implementing Two-Factor Authentication Would More Securely Authenticate Users to the System to Better Protect GSA Employee Travel and Financial Information

Authentication controls are used to verify the identity of a user, process, or device to allow access to resources in an information system. Office of Management and Budget (OMB) Memorandum M-07-16 requires that all Federal information systems only allow remote access with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access. CWGT began offering two-factor authentication with E2 in September 2008. At the time of our review, GSA had not yet selected two-factor authentication for its implementation of the E2 system. Currently, E2 users in GSA access the system by using user name and password; thus, authentication to the system is done based only on what the user knows. GSA's implementation of E2 does not augment authentication methods using either of the other two factors: (1) what the user has or (2) who the user is. Simple username and password authentication leaves users susceptible to attacks that are preventable with two-factor authentication, such as key stroke logging. One reason for the delay in implementing two-factor authentication for E2 is that the OCFO is waiting on the GSA Agency-wide solution for two-factor authentication. While current plans call for the GSA Chief Information Officer (CIO) to roll-out two-factor authentication in September 2009, implementing two-factor authentication Agency-wide has been delayed over the past few years. Until two-factor authentication has been implemented, it is easier for an unauthorized user to access, modify or disclose sensitive information in E2 solutions.

The FAS-PMO completed an eAuthentication risk assessment for E2, which recommended the use of Level 3 authentication for users with access to or authority over 20 or more user accounts, in September 2004. This level of authentication requires two-factor authentication of users with this type of privileged access. System administrators have access to the profiles of other users, which may contain PII. At a minimum, GSA should expedite implementation of two-factor authentication for E2 users with access to 20 or more user accounts.

Access to Procedures for Privileged Users Are Not Restricted to Those with a Need-to-Know

While authentication controls verify a user's identity, authorization controls establish what a user is authorized to do and what privileges a user should have in an information system. For E2, a system administrator (depending on his/her level) can manage users, configure major and minor customer settings and define routing rules and approvers. Our review identified that all system users, through the system help feature, had access to system administrator procedures rather than restricting them to only those with a need-to-know. According to a CWGT official, these procedures were not hidden because the E2 Knowledge Base[9] was deliberately designed to contain all aspects of the system that are available for E2 users and to allow all E2 users this

[9] The Knowledge Base is a database within E2 containing information related to all of the actions that are permitted within the system.

access. The CWGT official also stated that the system administrators' procedures in the E2 Knowledge Base were not hidden because only system administrators are able to actually perform the functions and because the Knowledge Base does not include procedures for performing Carlson-level system administrator functions, which controls the entire system. We also found that training procedures that include information on privileged system administer functions were available to those without a need-to-know, as these procedures were posted on GSA's Intranet and were made available to anyone with access to the Intranet, regardless of whether a person is an authorized E2 user. While granting knowledge of how to use E2 is necessary for using the system, by allowing access to privileged system administrators' procedures, a user may use explicit knowledge gained to devise a malicious attack by making unauthorized additions, modifications, or deletions to GSA's E2 data and/or processes. Subsequent to discussing our findings with security officials, the OCFO has removed the privileged training procedures from GSA's Intranet. However, to fully address this weakness, GSA should also ensure that access to privileged procedures within the system is restricted to those with a need-to-know.

Prompt Remediation of Configuration Management Vulnerabilities Could Reduce Risks from Known Vulnerabilities

System security officials have taken proactive steps to secure E2 system components, such as performing quarterly vulnerability scanning, and tracking and documenting any system changes. However, insecure configuration settings of system components have placed the confidentiality, integrity, and availability of the E2 system and its data at risk. While our testing did not identify any issues with the web application security, we found vulnerabilities with database hardening and system device configurations detailed in the sections that follow.

Database Security

GSA's IT Security Policy requires that all information systems be securely hardened and patched before being put into operation, and NIST SP 800-53 requires the organization to configure the security settings of information technology products to the most restrictive mode consistent with operational requirements. Additionally, GSA security guidance requires that the system enforce controls to ensure that the password for user accounts not be the same value as the username and that information systems should be designed to require passwords to be changed every 90 days. While E2 databases should have been securely configured to meet these requirements, our testing found two security vulnerabilities, one high level vulnerability and one medium level vulnerability, on the E2 Oracle database servers. Specifically, we found Oracle user accounts with the password the same as the user name and Oracle accounts with expired passwords. Security vulnerabilities found with the E2 databases were due to insufficient oversight of the contractor. Specifically, system security officials noted that the insecure database passwords may have resulted from a password reset by a database administrator. Because weak passwords provide one of the most common methods for gaining unauthorized system access, which could lead to a compromise of confidentiality, integrity, and or availability of the travel services provided by GSA's implementation of E2, the OCFO should work with the FAS-PMO to ensure the database is configured in accordance with GSA security guidance. Additional details of configuration management vulnerabilities identified with our technical database scanning are noted in Appendix E.

Network Security

As discussed previously, GSA's IT Security Policy requires all systems to be securely hardened before being put into operation. The policy also requires information systems to protect the confidentiality of transmitted sensitive information. Additionally, NIST SP 800-53 requires that federal information systems be securely configured to provide only the essential capabilities necessary to support organizational operations and that the organization promptly install newly released security updates after testing for adverse effects. Our network-based vulnerability testing identified that system hardening efforts taken by the security officials were not sufficient to ensure that all devices were appropriately hardened, as we found two high and two medium level vulnerabilities on 11 of the 17 system devices tested. Specifically, we identified that all unnecessary services had not been removed or turned off and that patches had not been applied in a timely manner. Unnecessary services running on the system and untimely patching of devices on the network leave the system vulnerable to denial of service, unauthorized access, and remote command execution of vulnerabilities. In order to address identified system device security weaknesses, system security officials should strengthen configuration management processes to ensure that non-essential services are disabled and that the software running on the networked servers are patched timely. Additional details of configuration management vulnerabilities identified with our technical network-based security scanning are noted in Appendix F.

GSA Should Specify if Approved Domain Is Required for Accessing E2

Under FISMA, approved websites with domains that identify government systems, including "*.gov*", "*.mil*", or "*.Fed.us*", should be used in performing agency functions to ensure a clear, unambiguous public notification of the Agency's involvement in or sponsorship of the website. FISMA and OMB have previously recognized a need to use other domains in certain limited, approved circumstances for proper performance of agency functions. GSA is allowing access to E2 through a *.com* website without an explicit written determination by the GSA Administrator of the need to use an unapproved domain to perform Agency travel functions, as E2 has been viewed as a commercial system and service purchased for government use rather than a government system. The efficient, effective, and consistent use of Federal agency public websites is important to promote a more citizen centered government and to provide added confidence, integrity, and quality to the information provided by Federal agencies over the Internet. The use of non-government domains could also increase risks of phishing[10] attacks where deception is used to play on the public's trust of the legitimate entity. To mitigate the risks associated with the Agency's external web presence, GSA should determine whether a Federal web domain is necessary for the proper performance of this Agency function.

Use of Secure Government E-mail Accounts When Resetting E2 User Passwords Could Reduce System Risks

According to the United States Computer Emergency Readiness Team (US-CERT), users should not use free e-mail service providers when messages may contain sensitive information. Since

[10] According to US-CERT, the United States Computer Emergency Readiness Team, phishing is the act of stealing personal information via the Internet for the purpose of committing financial fraud.

users are not paying for free e-mail accounts, the free e-mail service providers may not have a strong commitment to protecting the user from various threats and the security features they offer might not meet government standards. Our review found that current processes for resetting E2 user account passwords leaves the system open to undue risk. When an E2 user needs to reset their password, they are required to call the E2 Help Desk. However, when calling the Help Desk, a user can verbally give the Help Desk operator an e-mail address to have the reset password sent to, even if the e-mail address is not previously identified in the user's profile. Additionally, with GSA's implementation of E2, users are permitted to modify the primary e-mail address from their GSA e-mail address to an address provided by a free e-mail service, such as Yahoo!, Hotmail, or Gmail. The password reset e-mail provides a link to re-establish the user's security profile and requests that the user respond to two security questions, as long as the user has set up the security questions as part of their profile. If not, the user is not required to respond to any security questions to reset their password. CWGT officials indicated that the system was designed this way because some agencies do not use government e-mail addresses and that a business case would have to be developed, and a task order put in place, to require a system change. Further, there is no Agency guidance prohibiting the use of free e-mail services when resetting E2 user passwords, or transmitting PII. To address this issue, the OCFO should require that the transmission of sensitive information, including password resets, be restricted to a GSA e-mail address.

Next Steps

A November 18, 2008 Office of General Counsel (OGC) memorandum provided a legal opinion that addressed questions raised by the GSA Senior Agency Information Security Officer (SAISO) regarding whether or not specific IT systems that are currently included in the GSA-CIO's FISMA inventory qualify as "Federally-Controlled Information Systems." The legal opinion considered the E-Travel systems, NETWORX Operational Support Systems, GSA SMARTPAY information systems, WITS3 Operational Support System, and two project management systems used by PBS. In this memorandum, the OGC concluded that only the PBS project management systems qualify as FISMA systems, as defined by the Federal Acquisition Regulation (FAR). This legal opinion seems to view FISMA information security requirements as being applicable only to "Federally Controlled Information Systems" per the FAR as opposed to the FISMA definition of applicability to "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Therefore, it was considered a contract administration issue rather than a risk management challenge for GSA. Recent OMB feedback to the SAISO stated that systems that hold Federal data should comply with all FISMA requirements and that controls for these systems should be risk-based and within a reasonable cost for the benefit provided. With this informal correspondence on the question raised regarding contractor operated systems, OMB emphasizes that GSA should have a program for managing the risk with these types of systems. This should include such things as determining the risk and the controls that are needed and ensuring that all IT security controls are correctly listed in contracts and that there are methods for the agency to check that contractors are complying with those requirements on an on-going basis.

CONCLUSIONS

The OCFO and FAS-PMO have applied many of the management, operational, and technical controls established with FISMA and GSA's IT Security Program for E2, a "moderate" risk system that maintains travel and financial data, including PII. Our review of 99 of 171 specific security controls found the need for improvement in 11 of those controls, approximately 11% of controls tested. While Agency officials are taking actions to enhance security for E2, we found the need to strengthen specific management, operational, and technical controls to maintain the security of the system and its sensitive data.

Risk management practices can be improved by strengthening management controls to ensure that security controls required for and risks specific to GSA's implementation of E2 are considered and that that all needed risk assessment components have been addressed. We also found the need to establish an ISA/MOU for the E2/GDS interconnection. The Agency can enhance operational readiness by ensuring that background investigations for contractors are performed and that those contractors have completed annual security awareness training prior to granting them full access to the E2 system. Additionally, applying additional technical controls, such as implementing two-factor authentication and restricting access to privileged information on system administrative procedures, can strengthen system security. Opportunities also exist to strengthen technical controls by assessing whether the use of an approved web domain should be required for accessing E2 and whether use of a secure e-mail address for account password reset is needed. Finally, securely configuring E2 databases and other system components would help to ensure the protection of the system and its data. Strengthening management, operational, and technical controls, as noted in this report, can facilitate ongoing efforts to ensure that E2, and the sensitive travel and financial data it maintains, are adequately secured.

RECOMMENDATIONS

To better manage IT security risks with the GSA implementation of E2 and ensure the confidentiality, integrity and availability of this system and the data it maintains, we recommend that the Office of the Chief Financial Officer (OCFO) work with the Federal Acquisition Service (FAS) Program Management Office (PMO) and the Office of the Chief Information Officer (OCIO), to take actions to strengthen:

1. Management controls by:

    a) Ensuring that controls for and risks with GSA's implementation of E2, specific to the GSA IT systems environment, have been adequately addressed.
    b) Establishing a Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) for the E2 interconnection with the Global Distribution System (GDS).

2. Operational controls by:

    a) Obtaining assurance that an adequate process is in place and being used to effectively track the completion of background investigations and annual security awareness training prior to providing contractors with full access to GSA data.

3. Technical controls by:

    a) Identifying those users with privileged access and expedite implementation of two-factor authentication for those users.
    b) Restricting access to privileged procedures to those with a need-to-know.
    c) Ensuring that GSA-Chief Information Officer (CIO) hardening guides are applied.
    d) Disabling unnecessary functionality to eliminate the threat posed by providing non-essential services and ensuring that software running on the networked servers is properly patched to their most recent versions.
    e) Determining whether a *.com* domain is necessary for the proper performance of the operation of the E2 Solutions (E2) travel system, or whether an approved web domain, such as *.gov*, *.mil*, or *.Fed.us* should be used.
    f) Developing IT Security procedures to restrict the transmission of sensitive information, including password resets, to government e-mail addresses.

MANAGEMENT COMMENTS

Our recommendations are directed to the GSA-CFO and focus on specific improvements for management, operational, and technical controls needed to strengthen security for GSA's implementation of the e-Government Travel Services E2 Solutions system. The CFO generally agrees with our findings and recommendations, and a copy of the written management response to our draft report is provided in Appendix G. Included in the management comments are views from the FAS-PMO, who has responsibilities for ensuring that FISMA requirements are met for the government-wide E2 Solutions also offered by GSA to other Federal agencies. As discussed in our report, the GSA Office of the CFO is responsible for ensuring the implementation of adequate security controls for the Agency's implementation of the e-Government Travel Services E2 Solutions system as GSA's official travel management solution. With this FISMA security audit, we also considered the key role of the GSA Senior Agency Information Security Officer who is responsible, within the GSA IT Security Program, for ensuring that systems that hold Federal data comply with all FISMA requirements and that controls for these systems are risk-based and within reasonable cost for the benefit provided. Our position, as noted throughout the report, is that GSA's IT Security Program should ensure that risks are being managed with GSA e-Government systems, including this e-Government Travel Services E2 Solutions system. While some issues raised may require specific actions from the FAS-PMO for the government-wide e-Travel solution, our audit did not include a focused assessment of government-wide security requirements for e-Government systems or full capabilities of the broader e-Government Travel Services E2 Solutions system offered by the FAS-PMO. Included in the CFO's comments to our draft report is a response from the FAS-PMO that indicates disagreement related to two of our recommendations to the GSA-CFO.

Recommendation #1b calls for the GSA-CFO to work with the FAS-PMO and the GSA-CIO to establish a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) for the E2 Interconnection with the Global Distribution System (GDS). As indicated with the CFO's management response, the FAS-PMO disagreed with this recommendation, stating that the GDSx application interface is considered within the E2 System boundary and that CWGT does not directly connect to the GDS via a connection type that requires an ISA/MOU. We maintain that these agreements are needed to adequately secure GSA's systems and data under the provisions of FISMA. By gaining assurance that the FAS-PMO has established all needed MOUs/ISAs related to the government-wide solution provided to GSA, the CFO will be better equipped to manage security for GSA's implementation of E2. Attention to these critical agreements will also help the CFO to prevent, detect, deter, and recover from a compromise of GSA financial or sensitive travel data because of a security breach with an interconnecting system.

Recommendation #3e also calls for the GSA-CFO to work with the FAS-PMO and GSA-CIO to determine whether a *.com* domain is necessary for the e-Government Travel Services E2 Solutions system. In the CFO's management response, the FAS-PMO disagreed with this recommendation, stating that ETS vendors do not fall under the category of a Federal agency public website, as defined by OMB. We maintain the need for the CFO to take actions to address risks identified by our audit, including following criteria for a Federal agency public website since E2 is operated by an Agency, contractor, or other organization on behalf of the Agency. A decision as to whether or not it is acceptable to access E2 through a *.com* website rather than through a *.gov*, *.mil*, or *.Fed.us* website should be made to determine whether or not the Agency may be able to leverage potential security enhancements.

INTERNAL CONTROLS

As discussed in the objective, scope, and methodology section of our report, which is shown in Appendix A, the objective of our audit was to determine if GSA has implemented management, operational, and technical security controls to effectively manage specific risks with a travel and financial management system which holds PII in accordance with the Federal Information Security Management Act of 2002 (FISMA) and the Agency's Information Technology (IT) Security Program. If not, what additional actions are needed to better manage IT security risks for the system? As such, we assessed the effectiveness of implementation of the requirements of FISMA and the policies and procedures established with GSA's IT Security Program. This audit included a review of selected management, operational, and technical controls for "moderate risk" systems, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* Revision 2, December 2007. We did not test all controls required by NIST or detailed security requirements established with GSA's IT Security Program for E2. The Results of Audit and Recommendations sections of the report state, in detail, the need to strengthen specific management, operational, and technical controls with E2.

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY

This interim audit report on information security of the General Services Administration (GSA) implementation of the E2 Solutions (E2) system was conducted under an ongoing, broader scope audit that we commenced in June 2008. This broader scope audit was divided into two phases. The first phase involved a review of the implementation of select security controls established under the Federal Information Security Management Act of 2002 (FISMA) and GSA's Information Technology (IT) Security Program for GSA's implementation of E2. The second phase will assess GSA's implementation of E2 to determine how well the system is meeting management and user requirements and the extent to which the system has achieved intended goals and benefits associated with transitioning to an e-Government e-Travel system. We will also determine whether GSA's implementation of E2 provides for efficient, effective, accurate, and secure travel transactions, including protection of personally identifiable information (PII) and other sensitive data such as Agency financial and travel information. Results of the second phase of the audit will be issued in a separate report.

The objective of our audit of information security for E2 was to determine if GSA has implemented management, operational, and technical security controls to effectively manage risks inherent with a travel and financial management system which holds PII, in accordance with FISMA and GSA's IT Security Program. If not, what additional actions are needed to better manage IT security risks for the system? We focused our security review on the web applications, databases, and associated system devices utilized by GSA to access and utilize E2 to provide travel management services. We did not include in this audit an assessment of the effectiveness or efficiency of the system or its functions or the accuracy of the data the system maintains.

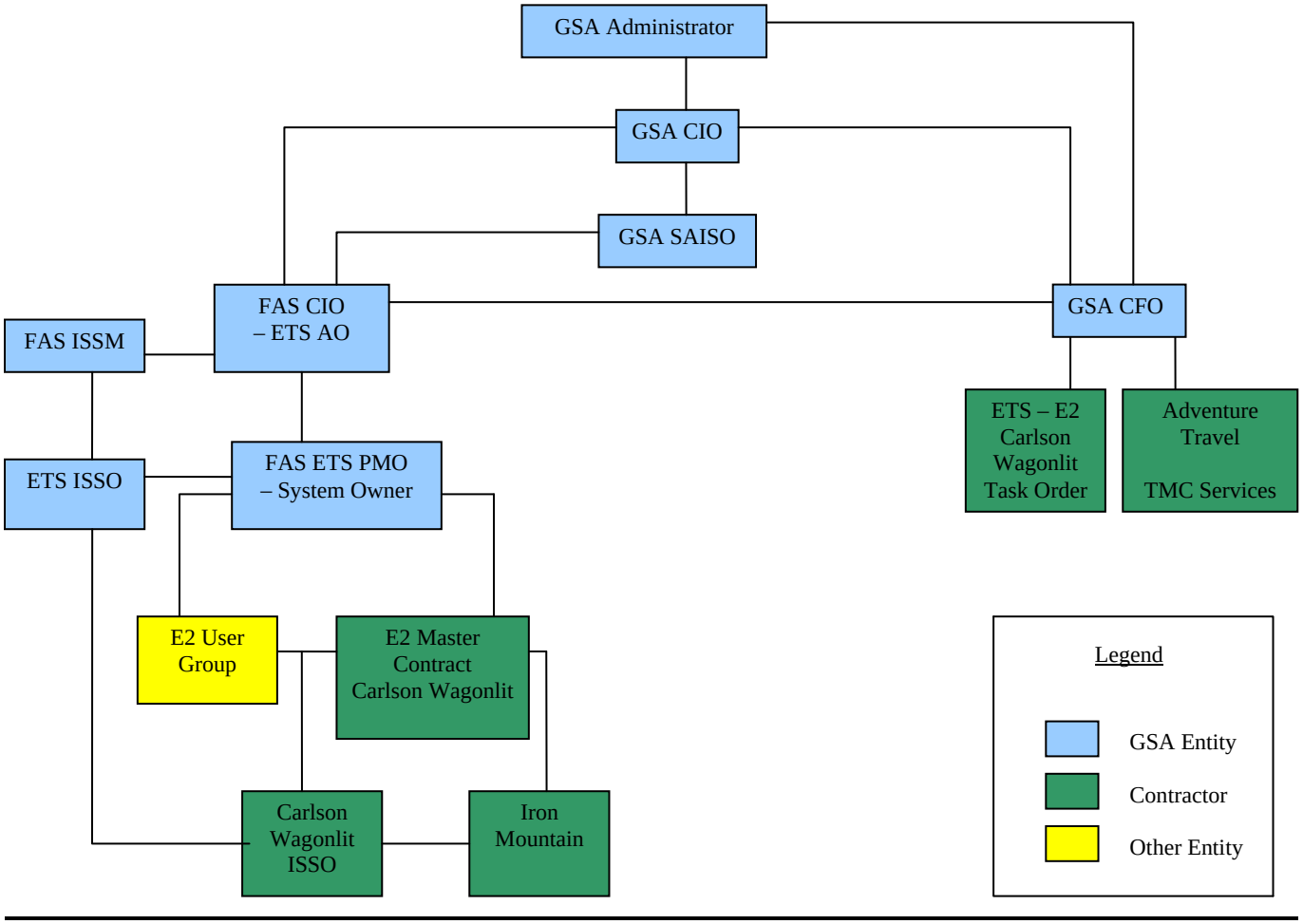
To gather information on E2, we met with system security officials, including the Federal Acquisition Service (FAS) Program Management Office (PMO) Information Systems Security Officer (ISSO) and the Carlson Wagonlit Government Travel (CGWT) ISSO. We also reviewed appropriate system security documentation, including the system certification and accreditation package, the interconnection security agreement between GSA and CWGT, memorandum of understanding, service level agreements, security incident reports transmitted to the US Computer Emergency Readiness Team (US-CERT), results of quarterly technical testing, quarterly updates to the system plan of action and milestones, security training records for individuals with significant security responsibilities, the eAuthentication risk assessment, and the privacy impact assessment. We performed a site visit to the primary data center in Plymouth, Minnesota on October 21, 2008, to the Disaster Recovery site in Omaha, Nebraska on October, 24, 2008, and to the Iron Mountain backup tape facility in Bloomington, Minnesota on October 23, 2008. We performed physical security reviews at all three sites and used commercially available tools and agreed upon procedures to test web application security, database security, and operating system security for the E2 system.

Our system tests included controls selected from each of the 17 families of controls identified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2 that establishes minimum information security requirements. Additionally, we reviewed applicable hardening and procedural guides published by the GSA Chief Information Officer and internal security procedures developed by the E2 contractor, CWGT. To assess controls for the system, we relied on information security legislation, policy, standards, procedures, and guidance, including the Office of Management and Budget (OMB) Circular A-130, Revised, Appendix III, *Security of Federal Automated Information Resources*, November 2000; OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, December 2004; OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007; OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*, August 2008; Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004; FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006; Federal Information Security Management Act of 2002 (FISMA); NIST special publications related to risk management, security planning, and certification and accreditation; *GSA Information Technology (IT) Security Policy*, CIO P 2100.1D, June 2007; and related GSA-CIO IT Security procedural guides, technical guides, and standards.

We conducted this performance audit in accordance with generally accepted government auditing standards between June 2008 and February 2009. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX B – SECURITY ROLES AND RESPONSIBILITIES RELATED TO GSA'S IMPLEMENTATION OF E2



FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX C - GSA-OIG E2 FISMA AUDIT PRELIMINARY OBSERVATIONS

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Access Controls (AC)	AC-2: Account Management	No reportable conditions identified.	
	AC-3: Access Enforcement	No reportable conditions identified.	
	AC-4: Information Flow Enforcement	No reportable conditions identified.	
	AC-5: Separation of Duties	No reportable conditions identified.	
	AC-6: Least Privilege	Access to privileged system administrative procedures has not been restricted based on a need-to-know.	The information system enforces the most restrictive set of rights/privileges/accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
	AC-7: Unsuccessful Login Attempts	No reportable conditions identified.	
	AC-8: System Use Notification	No reportable conditions identified.	
	AC-11: Session Lock	No reportable conditions identified.	
	AC-12: Session Termination	No reportable conditions identified.	
	AC-13: Supervision and Review	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Access Controls (AC) (cont.)	AC-17: Remote Access	While the Government-wide solution provides for the capability to implement two-factor authentication, GSA has not yet implemented two-factor authentication within its IT system environment.	The organization authorizes, monitors, and controls all methods of remote access to the information system.
	AC-18: Wireless Access Restrictions	No reportable conditions identified.	
	AC-19: Access Control for Portable and Mobile Devices	No reportable conditions identified.	
	AC-20: Use of External Information System	No reportable conditions identified.	
Awareness and Training (AT)	AT-2: Security Awareness	GSA officials with significant security responsibilities have been provided with security awareness training. We were unable to verify that all contractors with privileged system and/or database administration access have received security awareness training due to deficiencies with the contractor's system for tracking training.	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and annually thereafter.
	AT-3: Security Training	No reportable conditions identified.	
	AT-4: Security Training Records	We were unable to verify that all contractors with privileged system and/or database administration access have received role-based training due to deficiencies with the contractor's system for tracking training.	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Audit & Accountability (AU)	AU-3: Content of Audit Records	No reportable conditions identified.	
	AU-4: Audit Storage Capacity	No reportable conditions identified.	
	AU-5: Response to Audit Processing Failures	No reportable conditions identified.	
	AU-6: Audit Monitoring, Analysis, and Reporting	No reportable conditions identified.	
	AU-9: Protection of Audit Information	No reportable conditions identified.	
	AU-10: Non-Repudiation	No reportable conditions identified.	
Certification, Accreditation, and Security Assessments (CA)	CA-2: Security Assessments	No reportable conditions identified.	
	CA-3: Information System Connections	Risks with the GDS Interconnections to E2 did not appear to be assessed and managed within the C&A.	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Certification, Accreditation, and Security Assessments (CA) (cont.)	CA-4: Security Certification	GSA has not completed a Certification and Accreditation (C&A) of its implementation of E2, therefore, specific controls within GSA were not documented.	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
	CA-5: Plan of Action and Milestones	No reportable conditions identified.	
	CA-6: Security Accreditation	GSA has not completed a Certification and Accreditation (C&A) of its implementation of E2, therefore, specific controls within GSA were not documented.	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization *at least every three years* or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.
	CA-7: Continuous Monitoring	No reportable conditions identified.	
Configuration Management (CM)	CM-3: Configuration Change Control	No reportable conditions identified.	
	CM-4: Monitoring Configuration Changes	No reportable conditions identified.	
	CM-5: Access Restrictions for Change	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Configuration Management (CM) (cont.)	CM-6: Configuration Settings	The databases and networked devices were not configured in accordance with NIST guidance and GSA hardening standards. • Our automated vulnerability testing identified insecure configuration settings (insecure database accounts, unnecessary services, and untimely patching) for the database and operating system that could affect the confidentiality, integrity, and availability of GSA's data.	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.
	CM-7: Least Functionality	Networked devices were not configured in accordance with NIST guidance and GSA hardening standards.	The organization configures the information system to provide only essential capabilities.
	CM-8: Information System Component Inventory	No reportable conditions identified.	
Contingency Planning (CP)	CP-2: Contingency Plan	No reportable conditions identified.	
	CP-3: Contingency Training	No reportable conditions identified.	
	CP-4: Contingency Plan Testing and Exercises	No reportable conditions identified.	
	CP-5: Contingency Plan Update	No reportable conditions identified.	
	CP-7: Alternate Processing Site	No reportable conditions identified.	
	CP-10: Information System Recovery and Reconstitution	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Identification and Authentication (IA)	IA-2 User Identification and Authentication	No reportable conditions identified.	
	IA-4: Identifier Management	No reportable conditions identified.	
	IA-5: Authenticator Management	No reportable conditions identified.	
Incident Response (IR)	IR-2: Incident Response Training	No reportable conditions identified.	
	IR-3: Incident Response Testing and Exercises	No reportable conditions identified.	
	IR-4: Incident Handling	No reportable conditions identified.	
	IR-5: Incident Monitoring	No reportable conditions identified.	
	IR-6: Incident Reporting	No reportable conditions identified.	
Maintenance (MA)	MA-2: Controlled Maintenance	No reportable conditions identified.	
	MA-3: Maintenance Tools	No reportable conditions identified.	
	MA-4: Remote Maintenance	No reportable conditions identified.	
	MA-5: Maintenance Personnel	No reportable conditions identified.	
Media Protection (MP)	MP-2: Media Access	No reportable conditions identified.	
	MP-4: Media Storage	No reportable conditions identified.	
	MP-5: Media Transport	No reportable conditions identified.	
	MP-6: Media Sanitization and Disposal	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Physical and Environmental Protection (PE)	PE-2: Physical Access Authorizations	No reportable conditions identified.	
	PE-3: Physical Access Control	No reportable conditions identified.	
	PE-6: Monitoring Physical Access	No reportable conditions identified.	
	PE-7: Visitor Control	No reportable conditions identified.	
	PE-8: Access Records	No reportable conditions identified.	
	PE-9: Power Equipment and Power Cabling	No reportable conditions identified.	
	PE-10: Emergency Shutoff	No reportable conditions identified.	
	PE-11: Emergency Power	No reportable conditions identified.	
	PE-12: Emergency Lighting	No reportable conditions identified.	
	PE-13: Fire Protection	No reportable conditions identified.	
	PE-14: Temperature and Humidity Controls	No reportable conditions identified.	
	PE-15: Water Damage Protection	No reportable conditions identified.	
	PE-16: Delivery and Removal	No reportable conditions identified.	
Planning (PL)	PL-2: System Security Plan	No reportable conditions identified.	
	PL-3: System Security Plan Update	No reportable conditions identified.	
	PL-4: Rules of Behavior	No reportable conditions identified.	
	PL-5: Privacy Impact Assessment	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
Personnel Security (PS)	PS-2: Position Categorization	No reportable conditions identified.	
	PS-3: Personnel Screening	No reportable conditions identified.	
	PS-4: Personnel Termination	No reportable conditions identified.	
	PS-5: Personnel Transfer	No reportable conditions identified.	
	PS-6: Access Agreements	No reportable conditions identified.	
	PS-7: Third-Party Personnel Security	Delays in completing background investigations.	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.
	PS-8 Personnel Sanctions	No reportable conditions identified.	
Risk Assessment (RA)	RA-2: Security Categorization	No reportable conditions identified.	
	RA-3: Risk Assessment	An assessment of risk to E2, as implemented within GSA's IT system environment, has not been performed.	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).
	RA-5: Vulnerability Scanning	No reportable conditions identified.	

NIST 800-53 Control Family	NIST 800-53 Control	Observation (Condition)	Criteria
System and Service Acquisition (SA)	SA-2: Allocation of Resources	No reportable conditions identified.	
	SA-3: Life Cycle Support	No reportable conditions identified.	
	SA-4: Acquisitions	No reportable conditions identified.	
System and Information Integrity (SI)	SC-5: Denial of Service Protection	No reportable conditions identified.	
	SC-8: Transmission Integrity	No reportable conditions identified.	
	SC-9: Transmission Confidentiality	No reportable conditions identified.	
	SC-12: Cryptographic Key Establishment and Management	No reportable conditions identified.	
	SC-13: Use of Cryptography	No reportable conditions identified.	
	SC-17: Public Key Infrastructure Certificates	No reportable conditions identified.	
	SI-2 Flaw Remediation	No reportable conditions identified.	
	SI-3: Malicious Code Protection	No reportable conditions identified.	
	SI-4: Information System Monitoring Tools and Techniques	No reportable conditions identified.	
	SI-5: Security Alerts and Advisories	No reportable conditions identified.	
	SI-10: Information Accuracy, Completeness, Validity, and Authenticity	No reportable conditions identified.	
	SI-11: Error Handling	No reportable conditions identified.	

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX D – E2 SYSTEM INTERCONNECTIONS
APPENDIX E – DATABASE SECURITY RESULTS
APPENDIX F – NETWORK SECURITY RESULTS

Due to the sensitive nature of information contained in this appendix, only reports provided to system security officials and the GSA Senior Agency Information Security Officer contain detailed technical security assessment results in Appendices D-F. Requests for the details of the technical security assessment results should be referred to the Deputy Assistant Inspector General for Information Technology Audits at 703-308-1223.

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX G – MANAGEMENT COMMENTS

GSA

GSA Office of the Chief Financial Officer

July 24, 2009

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: KATHLEEN M. TURCO
CHIEF FINANCIAL OFFICER (B)

SUBJECT: Comments Re: Draft FY2009 Office of Inspector General Audit of the E2 Travel System Security Controls – Report No. A080180-2

Thank you for the opportunity to provide comments on the subject draft audit Report. As you know, the FAS-PMO is responsible for ensuring that FISMA requirements are met for the Government-wide E2 System and the Office of the Chief Financial Officer (OCFO) is responsible for ensuring the implementation of adequate security controls for the General Services Administration's (GSA) specific implementation of the E2 System. We generally concur with the audit recommendations for the subject audit and offer the following additional comments:

Management Controls

Recommendation 1a. - Reassess risks and related controls for GSA's implementation of E2.

> **Response**: The OCFO concurs with the recommendation and agrees to reassess the IT security risks relating to GSA's E2 implementation. We will will also ensure that sufficient controls are implemented to mitigate any major risks identified in accordance with FISMA requirements.

Recommendation 1b. – Establish a Memorandum of Understanding (MOU) and an Interconnection Security Agreement for the E2 Interconnection with the Global Distribution System.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

Response: The FAS-PMO does not concur with the audit recommendation because the GDSx application interface is considered within the E2 System boundary and merely provides access to Passenger Name Records in the Global Distribution System, which is external to the boundary of the E2 Solutions System. The interconnection to GDSx is a web services call that establishes a TSL connection over which the travel travel itinerary information is passed. The E2 Solutions web application establishes a separate TLS-enabled connection and initiates a web services call containing the the unique record locator in place of traveler personally identifiable data. As such, CWGT does not directly connect to the GDS via a connection type (as defined in NIST 800-47) that requires an ISA/MOU.

Operational Controls

Recommendation 2a. – Ensure that an adequate process for background investigations and annual security awareness training is in place and being followed prior to granting access to GSA data.

Response: The FAS-PMO concurs with this recommendation and is responsible for tracking background investigations and assuring annual security awareness training for ETS contractors with access to the ETS data base. The ETS PMO has aggressively worked to address security awareness training with each ETS provider. By the end of FY 2009, all ETS providers will have put in place a security awareness training program.

With regard to background investigations, the ETS PMO has been tracking background investigations. However, as with many government programs, there can be significant lag between the time that background investigation documentation is presented and the FPS response is received by the ETS PMO. The FAS Office of Administration is assisting the PMO in improving the process and assisting in the initial quality control of incoming background investigation documentation.

Technical Controls

Recommendation 3a. – Expedite implementation of two-factor authentication, if possible.

Response: The OCFO concurs fully with the intent of the recommendation on IT security grounds and will further explore the possibility of implementing two-factor authentication for GSA E2 System administrators within the OCFO, working in concert with the SAISO and the OCIO.

Recommendation 3b. - Restrict access to privileged procedures to those with a "need-to-know".

Response: The OCFO concurs with this recommendation and has already taken action to address this issue by removing such information from access on GSA's internal web site (i.e. InSite).

Recommendation 3c. - Ensure that GSA-OCIO hardening guides are applied.

Response: The FAS-PMO concurs with this recommendation and will take appropriate action to ensure that the hardening guides are applied effectively.

Recommendation 3d. - Disable unnecessary functionality on networked servers.

Response: The FAS ETS PMO concurs with this recommendation and will take steps to ensure that unnecessary functionality is disabled and that network servers are properly patched. The FAS OCIO also conducts quarterly white and black hat scans to detect deviations and tracks these deviations through the POA&M process until these issues are resolved.

Recommendation 3e. - Determine whether a .com domain is necessary for the E2 Solutions System.

Response: The FAS ETS PMO does not concur with this recommendation in its present form. OMB M-05-04 states that Federal agency public websites are: "information resources funded in whole or in part by the Federal government and operated by an Agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-Federal user group and support the proper performance of an agency function." Accordingly, because ETS vendors are: 1) not funded in whole or in part by the Federal Government and 2) do not present information or provide services to the public or a specific non-Federal user group, this recommendation is considered to be not germane to the E2 Solutions travel system.

Recommendation 3f.. - Develop IT security procedures to restrict the transmission of Sensitive information including password resets to Government e-mail addresses.

Response: The OCFO concurs with this recommendation and will put a process in place to restrict transmission of password reset emails to GSA e-mail addresses.

FY 2009 OFFICE OF INSPECTOR GENERAL
AUDIT OF THE E2 TRAVEL SYSTEM
SECURITY CONTROLS
REPORT NUMBER A080180/B/T/F09008

APPENDIX H – REPORT DISTRIBUTION

WITH APPENDICES D-F Electronic Copies

Office of the Chief Financial Officer (B) 4
- Chief Financial Officer 3
- Director, Office of Financial Management Systems 1

Federal Acquisition Service (Q) 5
- Commissioner 1
- Acting Director, Office of Travel and Transportation Services 1
- Authorizing Official 1
- Information Systems Security Manager 1
- Information Systems Security Officer 1

Office of the Chief Information Officer (I) 2
- Office of the Senior Agency Information Security Officer 1

WITHOUT APPENDICES D-F

Chief Human Capital Officer (C) 1
Internal Control and Audit Division (BEI) 1
Assistant Inspector General for Auditing (JA and JAO) 2
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F) 1
Deputy Assistant Inspector General for Acquisition Audits (JA-A) 1
Administration and Data Systems Staff (JAS) 1
Assistant Inspector General for Investigations (JI) 1
Audit Liaison, Office of the Chief Financial Officer (B) 1
Audit Liaison, Federal Acquisition Service (Q) 1