The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed

August 29, 2011

Reference Number: 2011-20-076

Phone Number | 202-622-6500
Email Address | TIGTACommunications@tigta.treas.gov
Web Site | http://www.tigta.gov

THE IRS2GO SMARTPHONE APPLICATION IS SECURE, BUT DEVELOPMENT PROCESS IMPROVEMENTS ARE NEEDED

Highlights

Final Report issued on August 29, 2011

Highlights of Reference Number: 2011-20-076 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) developed the IRS2GO mobile application for the Apple iPhone® and the Google Android® smartphones. The application was successfully released to the public on January 20, 2011, and 147,205 iPhone users and 178,773 Android users had signed up as of May 15, 2011, and March 1, 2011, respectively. Although the IRS2GO application is secure, enhancements in the development process could be made for future mobile applications to ensure taxpayer privacy and security.

WHY TIGTA DID THE AUDIT

This audit was initiated because the IRS2GO application was the first mobile application developed by the IRS, and it allows the user to check on the status of his or her tax refund and receive tax tips. Our overall objective was to determine whether the IRS adequately tested and secured the IRS2GO smartphone application.

WHAT TIGTA FOUND

The IRS2GO application adequately secures data communications and does not store sensitive or Personally Identifiable Information on the smartphone. The IRS2GO application is available only from the Apple App Store or the Android Market. Smartphone users should ensure they are downloading this application from one of these two sites.

TIGTA found that appropriate processes were not followed for using a nonapproved programming language and open source software in the development of the IRS2GO application. Management was aware of the requirement to request waivers, but advised it made a risk-based decision not to pursue waivers in consideration of time constraints for the project. However, the IRS could not provide any documentation of the risk-based decision and informed us that it was a verbal decision.

TIGTA also found that documents required to authorize releasing the IRS2GO application to the public were not obtained until after the application was released. While the IRS2GO application did not have any significant security issues when it was released to the public, using a system development approach that does not comply with Office of Management and Budget Circular A-130 regulations increases the risk that applications released to the public may contain security or privacy weaknesses.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Associate Chief Information Officer, Enterprise Services, should ensure that waivers are obtained prior to deployment when applicable, risk-based decisions are clearly documented, and updates to the Plan of Action and Milestones are addressed within the appropriate time period. In addition, the Associate Chief Information Officer, Enterprise Services, should coordinate the review of open source technologies for consideration of approval for use in future application development efforts and ensure that all system development activities follow an approach that is compliant with Office of Management and Budget Circular A-130.

The IRS agreed with all of TIGTA's recommendations. In developing future mobile applications, the IRS plans to obtain the appropriate waivers prior to deployment, generate appropriate documentation for any risk-based decision, timely address appropriate actions, and continue to review proprietary and open source technologies. The IRS also plans to adhere to the current limited-use approval process and the Office of Management and Budget Circular A-130 for future pilot innovative projects.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 29, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed (Audit # 201120023)

This report presents the results of our review of the IRS2GO smartphone application. The overall objective of this review was to determine whether the Internal Revenue Service (IRS) adequately tested and secured the IRS2GO smartphone application that allows taxpayers to check the status of their refunds. This audit was initiated because the IRS2GO application was the first mobile application developed by the IRS. This review addresses the major management challenge of Modernization of the IRS.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

Table of Contents

Abbreviations

ELC	Enterprise Life Cycle
IRM	Internal Revenue Manual
IRS	Internal Revenue Service

Background

Mobile phones have undergone several major developmental shifts since they first became available to the public. The first mobile phones were heavy and expensive to operate. True handheld cellular mobile phone technology became available in the United States early in the 1980's and provided access to voice communications only. Later versions added the capability of text messaging.

In the 2000's, mobile phones became increasingly similar to small computers, with their own operating systems. These phones not only provided voice and text communications, but also allowed users access to the Internet via built-in web browsers and had the capability of running small applications provided by the mobile phone manufacturer.

Currently, even more advanced mobile phones (hereafter called smartphones) like the Apple iPhone® and the Google Android® not only provide their users with voice, text, and web browsing capability, but also provide access to third-party applications with expanded capabilities such as access to Global Positioning Satellite data, driving directions, road hazards, and remote control of home appliances like web cameras and digital recorders for satellite and cable television systems.

The Internal Revenue Service (IRS) recognized the fact that today's smartphone users were not being fully served via the current IRS web site and traditional phone assistance to access IRS resources. Therefore, the IRS developed a smartphone application that would provide tax tips to the smartphone user and allow the user to check on the status of his or her tax refund.

The IRS named its application IRS2GO, and it was launched on January 20, 2011, for the Apple iPhone and the Google Android smartphones. Apple iPhone users can download the application from the Apple App Store, while Android users can download it from the Android Market. The IRS2GO application had signed up 147,205 iPhone users and 178,773 Android users as of May 15, 2011, and March 1, 2011, respectively.[1]

This review was performed at the Modernization and Information Technology Services organization's Cybersecurity and Enterprise Services offices in New Carrollton, Maryland, during the period February through June 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our

[1] The number of users signed up for a smartphone app changes as additional users download the app or users remove the app from their smartphone.

audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The IRS2GO Application Adequately Protects Data Transmissions and Personally Identifiable Information

The Internal Revenue Manual (IRM) requires that applications using the Internet for the transmission of sensitive information shall use virtual private networks,[2] application-level encryption, or another approved means to protect data. The transmission of nonpublic IRS information, such as a Social Security Number, from a department server over the Internet shall be protected using a secure protocol that provides Federal Information Processing Standards Publication 140-2 or later compliant cryptography to prevent unauthorized disclosure and recognize unauthorized changes during transmission. In addition, as a requirement for all systems used to enter, process, store, display, or transmit sensitive information, the IRS shall use only cryptographic modules that have been validated in accordance with Federal Information Processing Standards 140-2 or later.

When the taxpayer requests the status of his or her refund, the IRS2GO application requires the user to provide the Social Security Number of the account to be checked, the Filing Status shown on the return in question, and the amount of the refund that the taxpayer expected to get back on the return. We determined through our discussions and review of security testing documentation that the IRS2GO application is encrypting all communications between the smartphone and the IRS web servers that are processing the request for the status of the taxpayer's refund. In addition, the application does not store sensitive or Personally Identifiable Information on the smartphone, and the application disables the copy and paste functions so the information cannot be accessed or copied.

While the IRS2GO application is adequately securing taxpayer data, taxpayers should be careful not to save their sensitive information in a nonsecure manner elsewhere on their smartphones. The IRS application is available only from the Apple App Store or the Android Market. Therefore, taxpayers who desire to use the IRS application should ensure they are downloading the IRS2GO application from one of those two sites. Although the application is secure, we identified several issues related to the development process.

Apple iPhone Programming Tools Were Not Approved

The IRS developed Programming and Source Code Standards that establish standards and guidelines to promote the development of maintainable, portable, and reliable software

[2] See Appendix IV for a glossary of terms.

applications in all IRS used/approved languages. A list of authorized open source languages and libraries is available to developers, and a waiver process has been developed for those situations where products not on the list need to be used.

The IRS also established guidelines to coordinate the assessment, development, maintenance, and improvement of development controls. To manage deviations from these controls, a waiver must be obtained. These guidelines also require that:

- A record of all exceptions and deviations shall be maintained.
- There shall be no waivers or deviations from the controls established under the IRM without approval from the Software Quality Committee.
- All new weaknesses are entered into appropriate Plan of Action and Milestones within 1 month of identification for program-level weaknesses and those for Federal Information Processing Standards Publication 199 HIGH systems, and 2 months for weaknesses for other systems.

On February 28, 2011, the IRS issued interim IRM guidelines implementing a new risk-based decision process. According to the new risk-based decision policy, the IRS shall allow exceptions to its own information technology security policies based on suitable justification and a thorough assessment of evident and potential risks when a security weakness is discovered. There are only two acceptable reasons for a risk-based decision: the IRM requirement is technically or operationally not possible, or it is not cost-effective. Risk-based decisions shall be tracked in a Plan of Action and Milestones as part of a system's security authorization.

The IRS2GO iPhone application uses the Objective C programming language that is similar to the approved C++ and C languages. It also has many differences and is defined as a separate programming language. Additionally, the iPhone IRS2GO application uses an open source library that has not been authorized for application development.

The IRS2GO application underwent a security code review conducted by an outside contractor and a report of the results was issued on December 23, 2010. Although there were no security vulnerabilities identified, the report discusses the fact that Objective C and an open source library were in use for the iPhone IRS2GO application. The contractor also noted that a waiver would be required for the open source library prior to the release of the application to the Apple App Store. A Security Risk Assessment by the IRS Cybersecurity organization released in October 2010 included a comment that nonapproved technologies were being used for the Apple iPhone code and recommended that waivers be requested.

Management was aware of the requirement to request waivers for the application more than 2 months prior to the release of the application to the public, and despite the recommendations of both the contractor that performed the code review and the IRS Cybersecurity organization staff, the Enterprise Services organization did not request waivers for the use of these nonapproved technologies. Management advised the Treasury Inspector General for Tax Administration that

they made a risk-based decision not to pursue waivers in consideration of time constraints for the project; however, the IRS could not provide any documentation of the risk-based decision and informed us that it was a verbal decision. In March 2011, the IRS added the need to obtain waivers for the use of nonapproved open source technologies to the Plan of Action and Milestones.

While no significant security problems were identified, development of future smartphone applications should follow approved processes to avoid introducing unnecessary risk into the development process, which essentially could result in the development of vulnerable software.

Recommendations

Recommendation 1: The Associate Chief Information Officer, Enterprise Services, should ensure that waivers are obtained prior to deployment, when applicable; risk-based decisions are clearly documented at the time the decisions are made; and updates to the Plan of Action and Milestones are addressed within the appropriate time period.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Services will ensure that waivers are obtained prior to deployment of new mobile application, when applicable. In addition, the IRS will ensure proper documentation is generated for any risk-based decision based on IRS guidelines and appropriate actions are addressed timely.

Recommendation 2: The Associate Chief Information Officer, Enterprise Services, should coordinate with the Enterprise Architecture organization and the Quality Software Committee to review open source technologies for consideration of approval for use in future application development efforts.

> ***Management's Response:*** The IRS agreed with this recommendation. In accordance with current practices, Enterprise Services will ensure that future pilot innovative projects, such as IRS2GO, adhere to the established limited-use approval process. The Enterprise Architecture organization, the Quality Software Council, and other governing bodies will also continue to review proprietary and open source technologies to determine suitability for adoption into the IRS environment for future and current use.

The IRS2GO Application Was Made Available to the Public Prior to Receiving Authorization for Release

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individual based on the implementation of an agreed upon set of security controls. By accrediting an information system, an agency official accepts responsibility

for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. The Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, made a single person responsible for operational security or the authority to operate.

The IRS has a sophisticated Enterprise Life Cycle (ELC) development process that it uses for large application development projects. The ELC process is not suited for small application development projects like the IRS2GO application that take only a couple of months to go from planning to implementation. The IRS ELC Project Management office is working within the applications development offices to develop more streamlined lifecycle processes for smaller, faster paced developments. For this reason, the IRS piloted an agile project management approach to develop the IRS2GO mobile application. However, documents required to authorize releasing the IRS2GO application to the public were not obtained until after the application was released because the IRS followed a pilot development process instead of an approved formal ELC process.

- On January 20, 2011, version 1.0 of the IRS2GO application was made available to the public.
- On January 21, 2011, a minor change to the IRS2GO application resulted in version 1.01 being released.
- On January 25, 2011, the IRS Authorizing Official and the IRS2GO Information System Owner both gave their approval for the IRS2GO application to go live.
- On February 23, 2011, the approval to forgo the Privacy Impact Assessment requirement was signed.

While the IRS2GO application did not have any significant security issues when it was released to the public, using a system development approach that does not comply with Office of Management and Budget Circular A-130 regulations increases the risk that applications released to the public may contain security or privacy weaknesses.

Recommendation

Recommendation 3: The Associate Chief Information Officer, Enterprise Services, should ensure that all system development activities follow an approach that is compliant with Office of Management and Budget Circular A-130.

> ***Management's Response:*** The IRS agreed with this recommendation. In accordance with current practices, Enterprise Services will ensure that all future system development activities using an agile or (rapid) project management approach are compliant with or effectively address the intent of the Office of Management and Budget Circular A-130.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS adequately tested and secured the IRS2GO smartphone application that allows taxpayers to check the status of their refunds. To accomplish our objective, we:

I. Determined whether the IRS has developed adequate policies and procedures pertaining to developing and securing smartphone applications.

- A. Researched the IRS, Department of the Treasury, and National Institute of Standards and Technology guidelines for application development procedures to ascertain whether small applications like the IRS2GO application are covered.
- B. Interviewed the application developers and reviewed documentation to verify that the appropriate procedures and guidelines have been followed.
- C. Researched the responsibility that the IRS has toward protecting taxpayers from third-party applications that access IRS web services.

II. Determined whether the IRS2GO application adequately protects taxpayer Personally Identifiable Information.[1]

- A. Verified through documentation review and discussions whether data transmissions are securely encrypted between the smartphone and the IRS web servers.
- B. Verified through documentation review and discussions whether taxpayer information is not being stored on the smartphone unless there is a significant need to maintain that data and it is securely encrypted.

III. Determined whether the IRS thoroughly tested the IRS2GO application code before releasing it to the public.

- A. Reviewed the results of any code reviews performed by the application developers to ensure that coding issues were corrected or mitigated fully.
- B. Reviewed the results of any security testing performed by the Cybersecurity organization to ensure that all security issues were resolved or mitigated fully.

[1] See Appendix IV for a glossary of terms.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: the Enterprise Services organization's policies and procedures for developing small applications and performing security testing. We evaluated the controls by interviewing management and reviewing policies and procedures and relevant supporting documentation.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Director
Larry Reimer, Information Technology Audit Manager
Cari Fogle, Lead Auditor
Mark Carder, Senior Auditor
Daniel Oakley, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Chief Information Officer for Operations OS:CTO
Director, Privacy, Information Protection, and Data Security OS:P
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Director, Customer Service OS:CTO:AD:CS
Director, Web Services OS:CTO:ES:WS
Director, Security Risk Management OS:CTO:C:SRM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Glossary of Terms

Term	Definition
Agile Project Management	An iterative method of determining requirements for software and for delivering projects in a highly flexible and interactive manner, where deliverables are submitted in stages. One difference between agile and iterative development is that the delivery time in agile is in weeks rather than months.
Application-Level Encryption	Transport Layer Security and its predecessor, Secure Sockets Layer, are cryptographic protocols that provide communications security over the Internet. The Transport Layer Security protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, and instant messaging.
Cryptography	The practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include Automated Teller Machine cards, computer passwords, and electronic commerce.
Enterprise Life Cycle	Integrates the management, business, and engineering life cycle processes that span the enterprise to align its business and information technology activities. It generally refers to an organization's approach for managing activities and making decisions during ongoing refreshment of business and technical practices to support its enterprise mission.

Term	Definition
Federal Information Processing Standard Publication 140-2 Series	Issued by the National Institute of Standards and Technology to coordinate the requirements and standards for cryptography modules that include both hardware and software components. The cryptographic modules are produced by the private sector or open source communities for use by the Federal Government and other regulated industries that collect, store, transfer, share, and disseminate sensitive but unclassified information.
Federal Information Processing Standards Publication 199	Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Open Source Library	Libraries contain code and data that provide services to independent programs. This allows the sharing and changing of code and data in a modular fashion. Open source describes a broad general type of software license that makes source code available to the general public with relaxed or nonexistent copyright restrictions.
Personally Identifiable Information	Refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
Plan of Action and Milestones	The process of planning and identifying the tasks necessary to reduce the risks of each weakness found in an information technology system. It documents the remedial actions taken to address any deficiencies in the security policies and monitors the progress of corrective actions.

Term	Definition
Privacy Impact Assessment	The IRS conducts a Privacy Impact Assessment on information systems that collect Personally Identifiable Information. Performing Privacy Impact Assessments ensures that the public is aware of the information collected by the IRS about them, any impact these systems have on personal privacy is adequately addressed, and the IRS collects enough personal information to administer its programs and no more.
Security Authorization	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements for the system.
Sensitive but Unclassified Information	A designation of information in the Federal Government that, though unclassified, often requires strict controls over its distribution.
Virtual Private Networks	A secure way of connecting to a private Local Area Network at a remote location, using the Internet or any insecure public network to transport the network data packets privately, using encryption.
Web Server	Can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet.

Appendix V

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

AUG 03 2011

RECEIVED
AUG 3 2011

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed (Audit # 201120023) (i-trak #2011-23210)

Thank you for your review of the IRS2GO Smartphone Application. We appreciate the opportunity to respond to your draft audit report and to discuss earlier draft report observations with the audit team. We especially appreciate your willingness to be part of the team from the very beginning so you can better understand rapid development methodologies used for mobile applications such as IRS2GO in light of your standard TIGTA audit processes.

As this is the first mobile application developed by the Internal Revenue Service we recognize we have more work to do to ensure we fully document our work and receive necessary waivers on a more timely basis under our rapid development process. Our Enterprise Life Cycle Project Management office is working within the applications development offices to ensure that the approved practices under our new streamlined approach meets basic requirements for documentation but does not impede the rapid delivery of applications. It should be noted here that OMB Circular A-130 was written over 25 years ago with its most recent revision in 2000, before the advent of more modern web and mobile platforms. Nonetheless, the IRS will collaborate with TIGTA to effectively address the intent of the A-130 guidelines for safe and effective use of web and mobile platforms.

We also want to acknowledge here that, although we were given advanced verbal authorization to release the Smartphone application to the public, we received the written approval two days after the application was released. Going forward, we will ensure that we have supporting documentation prior to the release of any mobile application.

I also appreciate recognition that the IRS2GO application secures taxpayer data by encrypting all communication between the Smartphone and the IRS web servers, and that no security vulnerabilities were identified. I am pleased you acknowledged that the application does not store sensitive or Personally Identifiable Information on the Smartphone, and that the application disables the copy and paste functions, so the information cannot be accessed or copied.

We value your continued support and the assistance and guidance your team provides. We look forward to working with you on other mobile applications. If you have any questions, please contact me at (202) 622-6800 or Peggy Hueston at (202) 283-4915.

Attachment

Attachment

Draft Audit Report - The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed (Audit#201120023) (i-trak #2011-23210)

RECOMMENDATION #1: The Associate Chief Information Officer, Enterprise Services, should ensure that waivers are obtained prior to deployment, when applicable; risk-based decisions are clearly documented at the time the decisions are made; and updates to the Plan of Action and Milestones are addressed within the appropriate time period.

CORRECTIVE ACTION #1: We concur with this recommendation. The Associate Chief Information Officer, Enterprise Services will ensure that waivers are obtained prior to deployment of any new mobile application, when applicable. In addition, we will ensure that proper documentation is generated for anyrisk-based decision based on IRM guidelines and appropriate actions are addressed timely.

IMPLEMENTATION DATE: July 10, 2011 (completed)

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Associate Chief Information Officer, Enterprise Services, should coordinate with the Enterprise Architecture organization and the Quality Software Committee to review open source technologies for consideration of approval for use in future application development efforts.

CORRECTIVE ACTION #2: We concur with this recommendation. In accordance with current practices, the Associate Chief Information Officer, Enterprise Services, will ensure that future pilot innovative projects, such as IRS2GO, adhere to the established limited-use approval process. The Enterprise Architecture organization, the Software Engineering Council and associated governing bodies will continue to review proprietary and open source technologies to determine suitability for adoption into the IRS environment for current and future use.

IMPLEMENTATION DATE: June 14, 2011 (completed)

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Associate Chief Information Officer, Enterprise Services, should ensure that all system development activities follow an approach that is compliant with Office of Management and Budget Circular A-130.

Attachment

Draft Audit Report - The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed (Audit#201120023) (i-trak #2011-23210)

CORRECTIVE ACTION #3: We concur with this recommendation. In accordance with current practices, the Associate Chief Information Officer, Enterprise Services will ensure that all future system development activities using an agile (or rapid) project management approach are compliant with or effectively address the intent of the Office of Management and Budget Circular A-130.

IMPLEMENTATION DATE: July 10, 2011 (completed)

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.