Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot

September 24, 2013

Reference Number: 2013-20-108

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

Phone Number | 202-622-6500
E-mail Address | TIGTACommunications@tigta.treas.gov
Website | http://www.treasury.gov/tigta

BETTER COST-BENEFIT ANALYSIS AND SECURITY MEASURES ARE NEEDED FOR THE BRING YOUR OWN DEVICE PILOT

Highlights

Final Report issued on September 24, 2013

Highlights of Reference Number: 2013-20-108 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Bring Your Own Device (BYOD) is a popular trend in mobile computing that allows users to access network resources on their personal mobile devices, such as smartphones. While BYOD has the potential to provide organizations with cost savings, increased productivity, and improved employee satisfaction, mobile devices often need additional protection due to threats of theft and malware exposure. The IRS must ensure that implementing a BYOD program would be cost effective and that any increased risks to the privacy and integrity of taxpayer data can be mitigated.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of TIGTA's Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to evaluate the IRS's costs, administration, and security for its BYOD efforts.

WHAT TIGTA FOUND

The IRS has taken several noteworthy actions to implement its BYOD pilot, including taking a phased approach and considering security. Although it has spent more than $900,000 on mobility, the IRS has not developed a complete cost-benefit analysis to fully justify the implementation of the BYOD concept.

Federal-level guidance states that BYOD should be cost effective and that a cost-benefit analysis is essential. While the IRS did prepare a simple cost analysis that compared the estimated cost of BYOD to the cost of the IRS's existing mobility programs prior to starting the BYOD pilot, it was not updated with complete information on assumptions and costs. BYOD could provide significant benefits; however, these benefits are just conjecture until the IRS conducts a thorough cost-benefit analysis.

Additionally, increased attention is still needed to address security concerns related to the 460 users participating in the BYOD pilot. The IRS allows BYOD devices access to resources on the IRS network in addition to providing e-mail access, increasing the risk that privacy and taxpayer data could be compromised. The IRS also allows devices based on the Android™ operating system to participate in the BYOD pilot, even though these devices are more subject to malware than the Apple® devices tested in earlier phases. Audit trails and training also need to be improved.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that a cost-benefit analysis for BYOD is completed that complies with Federal guidance, ensure that BYOD users are allowed access to e-mail functions only, takes some additional steps before admitting Android devices into the BYOD pilot, retains and reviews audit trails in compliance with existing policies, and provides periodic training for BYOD participants on threats and recommended security practices specific to BYOD.

In its response to the report, the IRS agreed with four of five recommendations and proposed some corrective actions that it plans to take only if the BYOD pilot is expanded or funding is identified. The IRS disagreed with the recommendation to defer admitting Android devices into the pilot until a security risk assessment is completed.

TIGTA believes that some of the corrective actions proposed by the IRS are inadequate because they are contingent on BYOD expansion or additional funding. The relevant controls should be put in place for the existing BYOD effort, which does not have a clear end date and which is being used by hundreds of employees and devices within the production environment.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 24, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot (Audit # 201320008)

This report presents the results of our review of the Internal Revenue Service's (IRS) costs, administration, and security for its Bring Your Own Device efforts. This audit was initiated as part of the Treasury Inspector General for Tax Administration's Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

BYOD	Bring Your Own Device
IRS	Internal Revenue Service
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology

Background

Bring Your Own Device (BYOD) is a popular trend in mobile computing. BYOD programs allow users to access an employer's network resources on their personal mobile devices. For example, employees can use their personally owned smartphone, tablet,[1] and similar devices to stay connected to and access data from their organization's internal network. Employees tend to like BYOD because it allows them to use their own preferred device, and, if they are required to have a cell phone for work, it can allow them to carry only one device. Businesses and Government agencies are receptive to it because it has the potential to provide cost savings, increase productivity, and improve employee satisfaction. BYOD can provide cost savings if the organization's cell phone ownership, service, and/or support are reduced or discontinued. Additionally, BYOD participants who did not previously have an assigned smartphone report increased productivity because they can quickly address important e-mails while traveling or between meetings. Employees who chose to participate in BYOD reported high levels of satisfaction with the experience. However, achieving benefits is contingent on implementation details and workforce acceptance.

BYOD devices are subject to distinctive threats on two specific fronts—as mobile devices and as personally owned devices. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices, *e.g.*, desktop and laptop devices used only within the organization's facilities and on the organization's networks.[2]

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices.

A Government Accountability Office report highlighted some threats related to mobile devices.[3] Although the report related to threats to mobile devices in general, these concepts also apply in the BYOD situation in which employees use their own personal phones or devices to access Government resources. This report, issued in September 2012, provides the following information:

> *Threats to the security of mobile devices and the information they store and process have been increasing significantly. For example, the number of variants*

[1] A smartphone is a cell phone with built-in applications (commonly referred to as "apps"), access to the Internet, and the ability to add more apps. A tablet is a computer contained in a single panel that is operated through a touch screen.

[2] National Institute of Standards and Technology, Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).

[3] Government Accountability Office, GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged* (Sept. 18, 2012).

> *of malicious software, known as "malware," aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185 percent in less than a year […]. Cyber criminals may use a variety of attack methods, including intercepting data as they are transmitted to and from mobile devices and inserting malicious code into software applications to gain access to users' sensitive information. These threats and attacks are facilitated by vulnerabilities in the design and configuration of mobile devices, as well as the ways consumers use them. Common vulnerabilities include a failure to enable password protection and operating systems that are not kept up to date with the latest security patches.*

The more recent Juniper Networks Third Annual Mobile Threats Report estimated that mobile malware grew 614 percent between March 2012 and March 2013, with 92 percent of it directed toward Android™ devices. The report cautioned that due to a complex and distributed environment for mobile devices, rates represent only directional trends.

Another notable mobile device threat is the increase in thefts, especially of smartphones. Recent reports indicate that as many as 40 percent of robberies involve stolen cell phones, particularly smartphones. An October 2012 Associated Press report stated that this may have reached a level of almost 50 percent of robberies in San Francisco, California. In response to the growing theft problem, the Federal Communications Commission partnered with private companies to launch an initiative that consists of a series of practical solutions designed to combat cell phone theft. However, challenges to enforcement remain.

Financial and personal information, including tax-related information, are increasingly targeted by cybercriminals.

Some reports suggest that mobile device users are even more susceptible to falling victim to phishing attacks[4] than conventional computer users. Cybercriminals increasingly seek to obtain sensitive financial and personal information, including tax-related information, through phishing and other types of cyberattacks. That mobile device users may be more susceptible to such attacks raises security concerns, particularly when the devices are used to access the enterprise network.

In addition to the risks related to mobile devices, BYOD introduces an element of risk related to personal ownership and use. When the Government owns the device, the Government can control and update the device as needed, similar to laptops, and can restrict certain uses of the device, such as downloading suspicious software or visiting inappropriate websites. However, this is not the case for personally owned devices, which rely on individual initiative to implement operating system updates or to take security precautions. Because such restrictions do not apply to personally owned devices, the chances of downloading malware-infected software may be

[4] Phishing attacks trick individuals into disclosing sensitive personal information through deceptive computer-based means.

increased through such activities as visiting inappropriate sites, participating in gambling, downloading apps from third-party sites, or even using social media sites.

Employers can use a mobile device management (MDM) solution to help mitigate the risks involved with mobile devices. MDM allows an organization to manage and control any mobile device on its network. For example, MDM may be used to ensure that only authorized users access the internal network, enforce password usage, ensure communication encryption, or limit access to network applications. MDM and other technologies can mitigate risks associated with mobile devices participating in BYOD. MDM is a growing area, with an increasing number of vendors offering these types of products. Education on security dangers and how to increase security is also helpful in mitigating risks.

Federal-level guidance related to BYOD is developing along with this new technology. To provide some Federal-level guidance based on successful implementations of BYOD, in August 2012, the White House issued *A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*. In addition, the National Institute of Standards and Technology (NIST) has issued guidance related to mobile devices and is working on more guidance related to BYOD; however, as of June 3, 2013, this guidance has not yet been issued. The NIST warns that, like any new technology, smartphones present new capabilities but also a number of new security challenges. Smartphones and tablet devices have powerful capabilities and can be used for sending and receiving e-mail, browsing the Web, online banking and commerce, social networking, storing and modifying documents, remotely accessing data, recording audio and video, and navigating (as navigation aids). These devices are now mobile computers.

This review was performed with information obtained from the Information Technology User and Network Services, Strategy and Planning, and Cybersecurity organizations located in Lanham, Maryland; the Office of Privacy, Governmental Liaison, and Disclosure located in Washington, D.C.; and site visits to Information Technology offices in Oakland and San Francisco, California, and the Wage and Investment Division office in Walnut Creek, California, during the period November 2012 through July 2013. 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 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 Internal Revenue Service (IRS) is currently piloting a limited BYOD effort.[5] It uses an MDM solution to control access to the internal network and to limit risks associated with mobile devices. The MDM solution encrypts organizational data and enforces certain security settings on the personal device, but it does not control or otherwise interfere with using the personal side of the device. BYOD participants have access to e-mail, calendaring, and some web-based internal IRS applications. However, technical limitations prevent users from interfacing with many IRS internal systems.

The IRS has taken several noteworthy actions with respect to implementing its BYOD pilot, including taking a phased approach and considering security. However, the IRS has not developed a complete cost-benefit analysis to fully justify the implementation of BYOD within the IRS. Additionally, increased attention is still needed to address security concerns.

Actions Have Been Taken to Test and Implement Bring Your Own Device on a Limited Scale

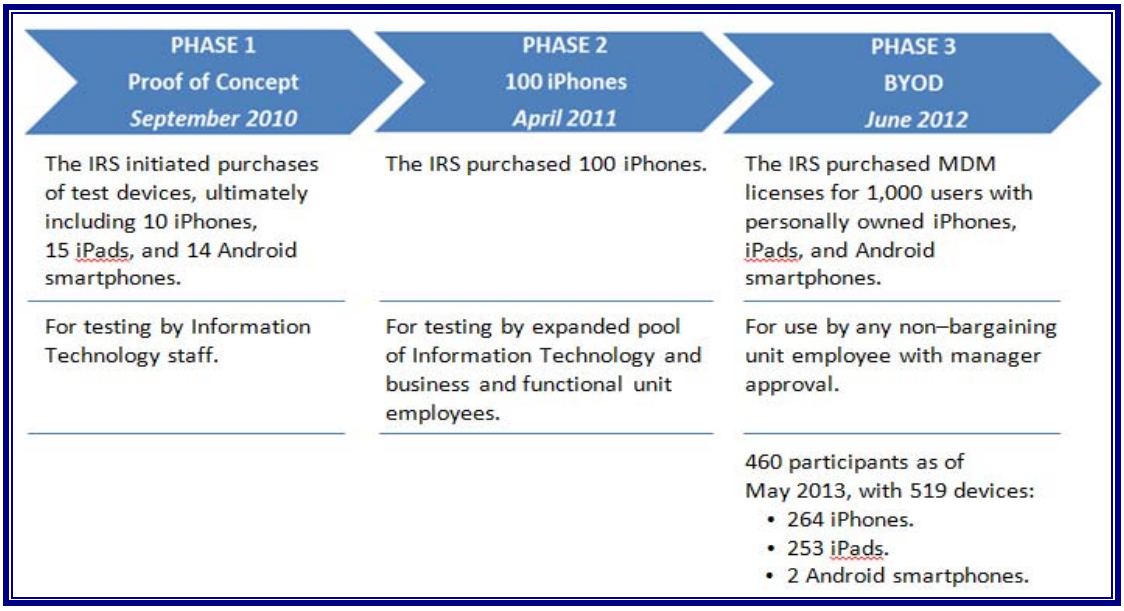
The driving force behind BYOD at the IRS has been investigating mobile technology that provides business value to employees and increasing employee productivity and satisfaction. To these ends, the IRS has proceeded toward BYOD in phases, which is in line with guidance in the White House BYOD Toolkit document that advises an incremental approach toward implementation.

Starting in September 2010, the IRS began a proof-of-concept effort to validate the technical feasibility of the MDM solution, which would allow the IRS to apply security settings on BYOD devices to mitigate risks. The proof-of-concept effort involved up to 39 Government-purchased smartphones and tablets and only involved testers from the Information Technology organization. In a second phase started in April 2011, the IRS purchased an additional 100 iPhone® devices, expanding the project to include non–Information Technology organization users. This phase was to help determine the business value of this solution on its own merits and in relation to the existing BlackBerry® mobile solution. Finally, in June 2012, the IRS started its third phase, a true BYOD program, when it purchased licenses for up to 1,000 devices to connect to the IRS network via the MDM solution. Initially, the program was limited to only devices

[5] The IRS currently refers to its BYOD pilot as a "technology demonstrator," which is meant to distinguish BYOD as a provisional initiative or prototype, thus differentiating it from formal pilots or large-scale information technology initiatives for which the IRS uses a well-established investment decision and enterprise lifecycle methodology. The word "pilot" is used in the report in a general sense for ease of understanding.

with iOS® operating systems (Apple® iPhone and iPad® devices) due to the enhanced security features available in conjunction with the MDM solution. The IRS rolled out the BYOD pilot to eligible employees[6] starting September 2012. In May 2013, the IRS opened the pilot to Android devices. Figure 1 illustrates the IRS's phased approach.

Figure 1: The IRS's Phased Approach to the BYOD Pilot



Source: Information provided by the IRS BYOD Project Team.

The IRS has made consideration of security an important feature of its mobility efforts with the implementation of the MDM solution for its BYOD program. The MDM solution used by the IRS was among those identified by the General Services Administration in May 2013 as a potential source of supply for MDM because the company understands Government requirements and provides a compliant encryption solution. Specifically, the MDM solution provides for a secure encrypted container for Government data on the device and secure communications with the IRS network. It enforces some basic controls over the security settings on the personal devices, such as requiring a passcode and enforcing a full device wipe after a certain number of unsuccessful passcode attempts. The MDM solution also provides the ability to identify devices, prevent jailbroken or rooted[7] devices from connecting, and send a signal to wipe information on the device. The IRS told us that it informally tested some key features of the MDM solution, such as its ability to wipe devices.

[6] Eligible employees were identified by the business and functional divisions and included only non–bargaining unit employees.

[7] Jailbreaking a device entails bypassing certain security features built into Apple iOS devices. Jailbreaking allows root access to the operating system and may allow a user to use apps besides those in the Apple App Store. Rooting is similar but applies to Android devices.

The Costs and Benefits of Bring Your Own Device Should Be Fully Evaluated

The IRS has not completed a full cost-benefit analysis for the BYOD pilot. While the IRS did prepare a simple cost analysis that compared the estimated cost of BYOD to the cost of the IRS's existing BlackBerry and cell phone programs prior to starting the BYOD pilot, the analysis was not updated with complete information on assumptions and costs. Consequently, as the pilot expanded, IRS managers relied on the original assumptions and cost projections in the analysis, which did not provide a sufficient basis for informed decision making.

The White House BYOD Toolkit document states that BYOD should be cost effective and that a cost-benefit analysis is essential.

The White House BYOD Toolkit document states that BYOD should be cost effective and that a cost-benefit analysis is essential. Detailed guidance on preparing a cost-benefit analysis is found in Office of Management and Budget Circular A-94, *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*. This circular describes elements of a cost-benefit analysis, including a policy rationale for the proposed program, a clear explanation of explicit assumptions and the rationale behind them as well as strengths and weaknesses, an evaluation of multiple alternative means of achieving program objectives, and a subsequent verification that anticipated benefits and costs were realized.

We found the following examples of inadequate assumptions or cost comparisons in the IRS's BYOD cost-benefit analysis.

- The analysis assumed that all users with IRS-provided phones would willingly choose to participate in BYOD when given a choice between BYOD and a Government-provided device. However, industry and Government reports indicate that only some employees will choose to participate. At another Federal organization, only 23 percent of the employees who had Government-provided devices chose to participate in BYOD when given the opportunity to do so. The IRS recently surveyed some of its employees currently provided a Government phone and, out of 58 respondents, only four indicated that they were willing to give up the Government phone for BYOD if keeping both a Government phone and a BYOD was not an option. Additionally, in the BYOD pilot phase, the IRS obtained 1,000 licenses to distribute throughout the business units but, as of May 2013, only 460 employees had taken advantage of the BYOD opportunity. The IRS used 519 of the 1,000 device licenses due to some employees having multiple devices.
- The analysis did not include continuing to provide and service about 190 Government-owned devices that are currently needed for a program that allows priority cell phone access for executives in case of emergency. The BYOD team noted in

another document that this program would not be terminated regardless of the BYOD implementation, so the analysis should have included it.

- The analysis overestimated the number of existing phone users and the total costs associated with the existing Government-provided BlackBerry and cell phone programs. The January 2013 IRS analysis was based on 20,000 total phone users, with 5,000 of those being BlackBerry users and the remaining 15,000 being cell phone users. However, when we requested information on the number of actual phone users in February 2013, the IRS told us that there were a total of about 14,800 users—about 4,300 BlackBerry users and about 10,500 cell phone users.

BYOD could provide significant benefits and even potential cost savings; however, these benefits are only conjecture until the IRS conducts a thorough, realistic cost-benefit analysis. While the White House BYOD Toolkit document states that a cost-benefit analysis of BYOD is essential, the IRS's own guidance does not require a detailed cost-benefit-type analysis for small technology demonstration projects such as the BYOD pilot; thus, such efforts have been limited.

The IRS estimates that it has spent more than $900,000 on its phased mobility efforts, including the BYOD pilot. While some issues existed with its analysis, the IRS estimated that a fully deployed program could cost about $3.9 million to start up and about an additional $2.2 million a year in ongoing costs for up to 20,000 users. This compares favorably to the IRS's estimate of about $7.6 million in annual costs for 20,000 users in the existing program. Even though the costs for the existing program appear to be overestimated, the IRS can realize some savings if participation is sufficient and security issues can be resolved. However, if users who are now provided phones as part of their work cannot be convinced to provide their own phones for work purposes, BYOD could end up as a costly "add-on" to the existing program.

Recommendation

Recommendation 1: The Chief Technology Officer should ensure that a cost-benefit analysis, in compliance with Office of Management and Budget Circular A-94, is completed for the existing BYOD pilot if it is continued as well as for any potential expanded BYOD program. The cost-benefit analysis should include realistic assumptions, especially related to participation rate. The team preparing the analysis should include employees with a financial background who are experienced in cost-benefit analysis.

> ***Management's Response:*** IRS management agreed with this recommendation and stated that when and if there is executive approval to continue or expand BYOD beyond a technical demonstration, the IRS will institute a cost-benefit analysis in compliance with Office of Management and Budget Circular A-94. The IRS pointed out that the existing BYOD is a technology demonstration and not a pilot.

Office of Audit Comment: We believe that the IRS should implement this recommendation for the existing BYOD program as well as any expanded version, regardless of whether it is called a technology demonstration or a pilot. Mobility efforts leading up to and including BYOD have cost the IRS over $900,000 so far, and the IRS had no estimated end date for the BYOD effort.

Increased Attention to Security Is Needed

Although the IRS did consider security and made it an important feature in implementing its mobility efforts, more should be done to ensure the security of the IRS network. Because the BYOD pilot takes place in the production environment, standard security controls should apply. The IRS allows BYOD devices access to resources on the IRS network in addition to providing e-mail access, increasing the risk that the privacy and integrity of taxpayer data could be compromised. The IRS also allows devices based on the Android operating system to participate in the BYOD pilot even though these devices are more subject to malware than the Apple devices tested in earlier phases. Lastly, audit trails and training also need to be improved.

Limiting access to only e-mail functions could help mitigate risks

Because the IRS is unable to fully implement Federal-level and IRS security guidance with respect to BYOD devices, we believe BYOD devices should only be allowed to access e-mail functions and should not be allowed to access other IRS network resources. This restriction would help limit the attack vector, should a security incident occur. We believe limiting BYOD to e-mail functions could have little impact on users, while providing greater security. A small judgmental[8] sample of BYOD users indicated that six out of seven users only used BYOD to read e-mails and not to access any other IRS applications. These results indicate that e-mail is the most valued BYOD function and that other applications add value to only some users or add only marginal benefit. Users could still use their Government-owned laptops to access the full range of network resources when necessary.

The IRS stated that users were given access to the IRS network for the BYOD pilot in order to evaluate the functionality and usability of mobile devices for business purposes. In terms of assessing the risks related to this increased functionality, the IRS stated that the MDM solution provides secure network browsing as part of its base product and that the Cybersecurity organization did not assert any unacceptable risk, provided the data were encrypted in motion and at rest, which the MDM solution achieves. The IRS further stated that one premise of the BYOD pilot is to take some risks and to give users access to what is needed in order to do their work using the MDM interface. The IRS stated that users need complete access to effectively test the MDM solution.

[8] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

To accomplish multiple security- and privacy-related purposes, the IRS is required to implement a range of information technology security policies. Federal guidance[9] requires enabling use of Personal Identity Verification credentials for controlling access to sensitive Government information. The IRS has not implemented this control with the BYOD pilot. The Federal Government is still working on guidance resolving issues related to applying this standard to mobile devices. Federal mandates also require a complex password in conjunction with a Personal Identity Verification credential to protect against unauthorized access to Government applications and services. **********2********** **********2********** **********2**********. The IRS currently is unable to enforce this requirement **********2********** on BYOD devices.

According to information from the U.S. Computer Emergency Readiness Team,[10] mobile phone security in general has not kept pace with traditional computer security. As smartphones become more popular and powerful, they have become an attractive target for attackers. Standard computer security measures such as firewalls, antivirus, and encryption are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as possible. Mobile devices are vulnerable to a range of attacks, including theft, software exploits, and phishing. Further, cybercriminals are motivated to find new types of exploits because of the valuable information mobile devices contain. Security researchers at the Georgia Institute of Technology have built a malicious charger that can inject persistent malware into current-generation iOS devices without jailbreaking the device. The security researchers stated that more motivated, well-funded adversaries could accomplish much more. The U.S. Computer Emergency Readiness Team cautioned that, given enough time, sophistication, and access to the device, any attacker could obtain information on the device.

The IRS commented that even if an attacker were able to gain access to the IRS network using a BYOD device, system controls would limit access to only those applications the employee was authorized to access. As such, if the employee did not have access to taxpayer data, the attacker would not have access either. However, if the employee did have access to taxpayer information, and a sophisticated attacker got access to the device, the attacker could also have that access.

The White House BYOD Toolkit document and the IRS's security policy state that devices must be configured and managed with information assurance controls commensurate with the sensitivity of the underlying data. Taxpayer and personal data are extremely sensitive information and deserve a high level of protection that is more important than providing convenience or modest cost savings. We believe that until the IRS completes a cost-benefit

[9] Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* directs agencywide use of Personal Identity Verification credentials for controlling access to sensitive Government information.
[10] *Cyber Threats to Mobile Phones*, revised February 6, 2013.

analysis that justifies a business need for a BYOD program, the IRS should limit BYOD access to e-mail functions only in order to mitigate risks.

Including Android operating system devices in BYOD increases the security risks

Android devices present more serious security risks than Apple devices in the BYOD environment. Multiple reports have documented increased malware targeted toward mobile devices, particularly toward Android devices. Malware presents serious risks that have not been adequately disclosed to management in formal documentation. Android devices are a bigger target for malware due to an open source operating system, a more lenient approval process for inclusion in the regulated app store, multiple third-party unregulated app stores, and lack of timely updates to correct operating system weaknesses.

In 2012, malware directed against Android devices increased significantly globally, and attacks are expected to increase in the United States as well. Malware may include keylogger or "spy" software. Keylogging software records keystrokes on the device and can automatically transmit data to a remote computer. Spy-type malware monitors device activity and can deliver Internet website addresses and upload data from a removable storage card. With the increase in attacks against all mobile devices, and Android devices in particular, malware presents a significant threat to device security

In August 2012, an IRS executive authorized the BYOD pilot, including Android devices, to conduct operations in the production environment, and the IRS began admitting Android devices into the program in May 2013. However, neither the authorization nor the other security documents referenced in the authorization, including a security technology review and a control impact assessment, discussed the security weaknesses specific to Android devices. The security technology review in July 2012 stated that the Android devices would be included in the BYOD pilot and that the IRS has the personnel and expertise to securely implement BYOD. However, the control impact assessment only discussed Apple devices and did not reference Android devices at all. No references were made in these documents to Android device weaknesses previously identified by the Cybersecurity organization, including malware targeting of Android devices. Based on the information discussed in the authorization, we are not convinced that the IRS executive had enough information to make an informed decision about the risks involved in bringing Android devices into the BYOD pilot.

It is unclear if an enterprisewide BYOD program would be either accepted by IRS users or cost effective without including Android devices. Nevertheless, the security issues should be acknowledged and mitigating controls identified.

Access audit trails are not retained or reviewed in compliance with IRS policy

According to the NIST, audit trails play an important role in computer security. Audit trails maintain a record of system processes and of user activity. One security purpose is to help system administrators ensure that the system or resources have not been harmed by hackers,

insiders, or technical problems. Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

**********2********** **********.[11] **********2**********
**********2**********
**********2**********.

Currently,**********2**********
**********2**********
**********2**********. However, the Cybersecurity organization has developed interim audit trail policy for the BYOD pilot. This interim guidance directs that **********2**********
**********2**********
*****2********. Additionally, because the BYOD operates in the production environment, we believe it should comply with existing IRS guidance related to audit trails. BYOD accesses involve hundreds of employees and are taking place in the production environment. The IRS should follow its existing guidance with respect to retaining and reviewing audit trails. If audit trails are not available or are not reviewed, unauthorized accesses may occur and not be detected.

Training would help inform users about mobile device threats

The Government Business Council and other sources recommend providing users with awareness training specific to the mobile environment. Office of Management and Budget Appendix III to Circular A-130, *Security of Federal Automated Information Resources*, requires that agencies ensure that users are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Appendix III to Circular A-130 also states that periodic refresher training should be required for continued access to the system. Further, the IRS's Cybersecurity organization has indicated that user training is important to enhance security related to mobile computing, and the Office of Privacy, Governmental Liaison, and Disclosure has indicated that communications with users about privacy and security issues should occur on a regular basis.

To bring its BYOD users up to speed on mobile device security, the IRS requires users to sign an online user agreement form that sets forth BYOD policies and addresses security issues. The IRS also provides a website where users can ask questions and see the responses from questions previously asked by other users. However, BYOD participants are not receiving periodic refresher training specific to BYOD threats and recommended security practices. While the IRS requires its employees to take annual computer security awareness training, the training is not

[11] Internal Revenue Manual 10.8.3, *Information Technology Security, Audit Logging Security Standards* (Sept. 16, 2011).

specifically targeted toward mobile device security. However, it could be improved to provide the ongoing security training that BYOD participants should receive.

The Government Business Council states that lapses in judgment or forgetfulness are unavoidable. A Telework Exchange survey[12] found that one in three Federal employees who use their personal smartphone for work do not even have password protection on their phones. Smartphone users may be even more susceptible to phishing than regular computer users. Currently, the IRS has no assurance that users are knowledgeable about elevated loss and theft rates, how to identify potentially dangerous apps, and other mobile-related device security issues.

Recommendations

The Chief Technology Officer should:

Recommendation 2: Ensure that BYOD users are allowed access only to e-mail functions in most cases and ensure that any users provided additional access to IRS network resources demonstrate a compelling business need for that increased access, especially considering that laptops already have full functionality on the IRS network.

> ***Management's Response:*** IRS management agreed with this recommendation. Access to additional IRS resources will use the same MDM secure container solution, ensuring complete isolation of IRS resources from the rest of the personal device, and be provided as business needs for the access are demonstrated.
>
> ***Office of Audit Comment:*** Although IRS management agreed with this recommendation, they do not plan to implement corrective action until November 2014. We believe that the IRS should implement this recommendation immediately for the existing BYOD participants and limit their BYOD access to e-mail functions only, unless a business need for further access has been demonstrated, in order to mitigate the risk of IRS sensitive data being compromised.

Recommendation 3: Defer admitting Android devices into a BYOD pilot or program until a security risk assessment has been completed that thoroughly addresses the malware and other risks associated with Android devices and the assessment has been reviewed and the risks accepted by executive management.

> ***Management's Response:*** IRS management disagreed with this recommendation. The IRS stated that BYOD is a technology demonstration and the IRS is evaluating various devices through the controlled secured environment of its MDM. IRS executive management reviewed the Cybersecurity Mobile Computing Security Technology Review and issued an authorization to conduct a BYOD technology demonstration which includes Android devices.

[12] *The 2013 Digital Dilemma Report: Mobility, Security, Productivity—Can We Have It All?* (Jan. 15, 2013).

Office of Audit Comment: We acknowledged in the report that both a security technology review and an authorization for BYOD were completed. However, there was no indication that the risks related to Android devices compared to Apple devices were disclosed to the authorizing official. We continue to believe that additional risk information on Android should be provided to IRS executives because neither the Cybersecurity Mobile Computing Security Technology Review nor other documents referenced in the authorization described the malware and other risks related to Android devices.

Recommendation 4: Ensure that the existing IRS policy related to audit trails is followed, **********2**********
**********2**********.

Management's Response: IRS management agreed with this recommendation. The MDM has built-in facilities to accumulate an audit log of access attempts, and the IRS believes these built-in capabilities are sufficient while BYOD is a technology demonstration. The IRS will investigate a method with the MDM server to **********2**********. In the event that the technology demonstration is adapted into a production system, all IRS policies regarding audit trails will be applied accordingly per the Enterprise Life Cycle.

Office of Audit Comment: The IRS stated that, if it expands the existing BYOD effort, it will investigate how to retain audit trails. We continue to believe that 1) the IRS should retain the audit trails in compliance with existing IRS policy for the current BYOD effort and not wait until the effort is further expanded and 2) the IRS should also review the audit trails daily. These controls should be implemented for the existing BYOD technology demonstration/pilot since there was no specified end date to the effort, and it already operates in the production environment with access to operational IRS systems and live data. At present, hundreds of employees and devices have access to IRS resources through their BYOD devices.

Recommendation 5: Provide periodic refresher training for BYOD participants that clearly explains the risks associated with personal mobile devices, how these can potentially expose the IRS network to unauthorized accesses and malware, the consequences of such breaches, and how to prevent or reduce the possibility of causing such a security breach.

Management's Response: The IRS agreed with this recommendation contingent on funding. If the decision is made to continue the existing technology demonstration or expand the program, the IRS will develop security training materials for BYOD participants that clearly explain the additional security threats associated with personal mobile devices and IRS data as well as best practices to mitigate these threats and reduce risks to agency information and resources.

Office of Audit Comment: Although IRS concerns related to funding are understandable, we continue to believe that all BYOD participants should be provided this information in some form on a regular basis to help mitigate security risks associated with BYOD.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the IRS's costs, administration, and security for its BYOD efforts. To accomplish this objective, we:

I. Determined if the IRS evaluated the costs and benefits of BYOD prior to and based on the results of the pilot and if actual costs and benefits are being adequately captured during the pilot.

- A. Obtained cost-benefit guidance for Federal projects, such as Office of Management and Budget guidance.
- B. Obtained cost-benefit analyses that the IRS has conducted related to BYOD and any necessary supporting documents.
- C. Interviewed IRS officials regarding methodology for the cost-benefit analysis and how ongoing costs and benefits are being captured.
- D. Assessed if key costs and benefits were adequately accounted for in the IRS's estimates and in the ongoing pilot.

II. Determined if the IRS BYOD program is being effectively administered.

- A. Interviewed IRS officials regarding how the program is administered.
- B. Reviewed helpdesk requests related to BYOD and the MDM solution to identify issues that have been reported and how they were resolved.
- C. Reviewed the inventory of devices and participants for potential issues, such as low participation rates.
- D. Determined if the IRS infrastructure provides the necessary functionality for BYOD hardware and software and risks of expanding the program.
- E. Determined if BYOD end user-related policies and procedures are effective and in accordance with Federal guidance and best practices.

III. Determined if IRS BYOD-related policies are sufficient to protect IRS data and if the policies have been effectively implemented in accordance with Federal policy.

- A. Obtained Governmental guidance and industry best practices related to BYOD (including mobile devices in general) and determined if IRS policies are in compliance with the NIST and other relevant guidance (including password, cryptographic, and Homeland Security Presidential Directive 12 guidance).

B. Determined if access controls and identification and authentication controls are effectively implemented. We selected a small judgmental sample[1] of seven IRS employees who were participating in BYOD and were co-located with the audit team and observed MDM operation on the personal devices. In May 2013, there was a total population of 460 BYOD users.

C. Determined if data protection controls are effectively implemented including controls related to encryption, passwords, connections, and data flow between BYOD components.

D. Determined if configuration management controls are effectively implemented related to system requirements, the MDM solution, device settings, and malware protection.

E. Determined if incident response controls are implemented effectively including the ability to detect jailbreaking,[2] unauthorized access attempts, or malware; the ability to wipe devices; and the ability to collect and review audit logs.[3]

F. Determined if employees should have access to the IRS intranet through BYOD, considering risks and other factors, and if this can be limited if necessary.

G. Determined if the program should be expanded to include Android devices.

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: Federal guidance and industry best practices related to cost, administration, and security on pilot technology projects and BYOD. We evaluated these controls by reviewing White House guidance on BYOD; Office of Management and Budget Circular A-94 *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*; Internal Revenue Manual 10.8.3, *Information Technology Security, Audit Logging Security Standards*; and other IRS, NIST, and industry guidance related to mobile devices. We also interviewed IRS Information Technology organization management in the Cybersecurity, User and Network Services, and Risk Management organizations as well as other IRS offices with duties related to BYOD. We interviewed and observed seven IRS employees as they operated their BYOD devices.

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.
[2] Jailbreaking a device entails bypassing certain security features built into Apple iOS devices. Jailbreaking allows root access to the operating system and may allow a user to use apps besides those in the Apple App Store. Rooting is similar but applies to Android devices.
[3] We used criteria for systems categorized as Moderate using criteria in NIST Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent T. Sagara, Director
Jody Kitazono, Audit Manager
Mary Jankowski, Lead Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Larry W. Reimer, Information Technology Specialist

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Technology Officer OS:CTO
Director, Privacy, Governmental Liaison, and Disclosure OS:P
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Director, Architecture and Implementation OS:CTO:C:AI
Director, Financial Management Services OS:CTO:SP:FM
Director, Investment Planning and Management OS:CTO:SP:IPM
Director, Business Planning and Risk Management OS:CTO:SP:RM
Director, Service Planning and Involvement OS:CTO:UNS:SPI
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: Chief Technology Officer OS:CTO

Appendix IV

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

September 9, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot - Audit # 201320008 (e-trak #2013-46364)

Thank you for the opportunity to review and respond to the subject draft audit report.

We appreciate TIGTA's concerns about the Bring Your Own Device (BYOD) technology demonstrator as acknowledged in your draft report. The BYOD technology demonstrator explores the full possibilities of mobile device options for IRS employees. We consider some of the recommendations in your report more appropriate for a BYOD program in production. While BYOD remains in an exploratory mode, we will continue to evaluate the pros and cons of the technology with due diligence to data security and cost effectiveness. Our responses to the specific recommendations in the report are attached.

We are committed to continuously improving our information technology systems and processes. We value your continued support and the assistance and guidance your organization provides. If you have any questions, please contact me at (202) 622-6800, or a member of your staff may contact Lisa Starr, Senior Manager of Program Oversight (240) 613-4336.

Attachment

Attachment

Draft Audit Report - Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot (Audit # 201320008) (e-trak# **2013-46364**)

RECOMMENDATION #1: The Chief Technology Officer should ensure that a cost-benefit analysis, in compliance with Office of Management and Budget Circular A-94, is completed for the existing BYOD pilot if it is continued, as well as for any potential expanded BYOD program. The cost-benefit analysis should include realistic assumptions, especially related to participation rate. The team preparing the analysis should include employees with a financial background who are experienced in cost-benefit analysis.

CORRECTIVE ACTION #1: IRS agrees that when and if there is executive approval to continue or expand BYOD, beyond a technical demonstration the IRS will institute a cost-benefit analysis in compliance with Office of Management and Budget Circular A-94. The existing BYOD is a technology demonstration and not a pilot.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, User and Network Services.

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: The Chief Technology Officer should ensure that BYOD users are allowed access only to e-mail functions in most cases, and ensure that any users provided additional access to IRS network resources demonstrate a compelling business need for that increased access, especially considering that laptops already have full functionality on the IRS network.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The goal of enterprise mobility is to improve employee productivity by allowing greater access to enterprise resources from mobile devices while maintaining the overall security posture of the organization. The BYOD technology demonstration utilizes the Good for Enterprise Mobile Device Management (MDM) secure container solution, coupled with the IRS firewall protection, to ensure complete separation between personal data and IRS resources and primarily provides email functions to BYOD users. Access to additional IRS resources will utilize the same Good for Enterprise secure container solution, ensuring complete isolation of IRS resources from the rest of the personal device, and be provided as business needs for the access are demonstrated.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, User and Network Services

Attachment

Draft Audit Report- Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot - Audit# 201320008 (e-trak #2013-46364)

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

RECOMMENDATION #3: The Chief Technology Officer should defer admitting Android® devices into a BYOD pilot or program until a security risk assessment has been completed that thoroughly addresses the malware and other risks associated with Android® devices, and the assessment has been reviewed and the risks accepted by executive management.

CORRECTIVE ACTION #3: The IRS disagrees with this recommendation concerning deferral of Android® devices. This is a technology demonstration and the IRS is evaluating various devices through the controlled secured environment of Good for Enterprise Mobile Device Management (MDM). IRS Executive Management reviewed the Cybersecurity Mobile Computing Security Technology Review and issued an Authorization to Conduct BYOD technology demonstration which includes Android devices.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, User and Network Services.

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4: The Chief Technology Officer should ensure that the existing IRS policy related to audit trails is followed, **********2********** **********2**********.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The Good Mobile Device Management server has built-in facilities to accumulate an audit log of access attempts, and the IRS believes these built in capabilities are sufficient while BYOD is a technology demonstration. The IRS will investigate a method within the Good Mobile Device Management Server**********2**********. In the event that the technology demonstration is adapted into a production system, then all IRS policy regarding audit trails will be applied accordingly per the Enterprise Life Cycle (ELC).

IMPLEMENTATION DATE: February 25, 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, User and Network Services

Attachment

Draft Audit Report - Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot (Audit # 201320008) (e-trak**# 2013-46364**)

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

RECOMMENDATION #5: The Chief Technology Officer should provide periodic refresher training for BYOD participants that clearly explain the risks associated with personal mobile devices, how these can potentially expose the IRS network to unauthorized accesses and malware, the consequences of such breaches, and how to prevent or reduce the possibility of causing such a security breach.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation contingent on funding. If the decision is made to continue the existing technology demonstration or expand the program, we will develop security training materials for BYOD participants that clearly explain the additional security threats associated with personal mobile devices and IRS data, as well as best practices to mitigate these threats and reduce risk to agency information and resources.

IMPLEMENTATION DATE: February 25, 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

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