

---

---

**TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION**



***Additional Security Is Needed for  
Access to the Registered User Portal***

**March 31, 2010**

**Reference Number: 2010-20-027**

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:**

1 = Tax Return/Return Information  
2(f) = Risk Circumvention of Agency Regulation or Statute

---

---

**Phone Number** | **202-622-6500**  
**Email Address** | **[inquiries@tigta.treas.gov](mailto:inquiries@tigta.treas.gov)**  
**Web Site** | **<http://www.tigta.gov>**



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

March 31, 2010

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER  
COMMISSIONER, WAGE AND INVESTMENT DIVISION

*Michael R. Phillips*

**FROM:** Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Additional Security Is Needed for Access to the  
Registered User Portal (Audit # 200920014)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) established effective access and audit trail controls for the Registered User Portal (RUP), which allows access to the IRS' e-Services<sup>1</sup> suite of applications, to protect taxpayer data from unauthorized disclosure. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2009 Annual Audit Plan and was part of our statutory requirement to annually review the adequacy and security of IRS technology.

### *Impact on the Taxpayer*

The use of the Internet is an integral part of the IRS' mission to deliver top quality service to all taxpayers. The IRS developed the RUP to help accomplish this mission. The RUP serves as the entry point for web access to e-Services applications and provides outside tax professionals with the ability to submit and retrieve tax-related information and electronically file (*e-file*) tax returns. Because these external users can access taxpayer data, modify electronic tax returns prior to transmitting them to the IRS, and download taxpayer data to their computers, access controls at the RUP are critical to minimize the risk of unauthorized access to taxpayers' personal tax data.

---

<sup>1</sup> See Appendix IV for a list of e-Services products.



*Additional Security Is Needed for  
Access to the Registered User Portal*

Synopsis

The RUP and e-Services applications allow the IRS to become more efficient and make tax filing easier. During the 2008 Filing Season,<sup>2</sup> 58 percent of all tax returns, nearly 90 million of the 155 million tax returns filed, were received electronically. However, the RUP and e-Services applications also pose risks to the security of taxpayers’ personal data. To mitigate the risks, the IRS implemented several access controls. For example, the RUP automatically disables a user account after three unsuccessful logon attempts, passwords are masked to prevent the passwords from being viewed when typed, and the RUP displays a banner to warn persons attempting to gain access that illegal attempts to log on to the system could lead to criminal prosecution. Although some access controls are in place, several other required controls were not implemented.

- Suitability checks are not performed on all users who *e-file* tax returns and access taxpayer data. The IRS allows principals and responsible officials at tax preparation firms to delegate their access rights to other individuals. These “delegates” may be members of the firm or persons with whom the firm has a business relationship and do not undergo a suitability check. A principal or responsible official also has the ability to delegate a “Principal Consent” right that allows the delegated user to propagate his or her access rights to other individuals.
- The IRS did not always follow its procedures for approving *e-file* applicants who failed the criminal background part of their suitability check. \*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*<sup>3</sup> \*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\* . IRS procedures do not specify which IRS office has the final authority to approve or disapprove an *e-file* applicant’s request to participate in the *e-file* program when an applicant fails his or her criminal background check.
- Limitations in the Third Party Data Store, which is used to record and monitor information about individuals who have applied to participate in the *e-file* program, prevent this system from posting the complete results of the systemic tax compliance check that is performed on an applicant’s spouse. Therefore, the spouse’s tax compliance check is performed manually, which is inefficient and increases the risk of human error.
- The RUP was not configured to disable and remove users’ access accounts in accordance with IRS security policies and procedures. Systems are required to disable inactive

<sup>2</sup> The period from January through mid-April when most individual income tax returns are filed.

<sup>3</sup> The IRS *e-file* program allows individuals to submit tax form data over the Internet.



## *Additional Security Is Needed for Access to the Registered User Portal*

accounts after 45 days and remove the accounts after 60 days.<sup>4</sup> Inactive accounts unnecessarily increase the opportunity for malicious individuals to gain access to taxpayer data through an unused account. Rather than implement the control to disable inactive accounts after 45 days, the IRS set the control to 720 days. In addition, the IRS did not implement a control to remove inactive accounts. The controls were not established because the IRS wanted to accommodate the users, many of whom have only a seasonal need to use the RUP.

- Required password controls were not implemented, and some individuals were using their Social Security Number as their username. The Office of Management and Budget<sup>5</sup> advised agencies in May 2007 to avoid or reduce the use of Social Security Numbers as personal identifiers.
- The IRS did not implement the control to \*\*\*\*\*2\*\*\*\*\* and does not analyze the RUP audit logs to detect unlawful or unauthorized activities.

### *Recommendations*

To ensure taxpayer data are safeguarded, we recommended the Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, 1) require suitability checks on delegated users who *e-file* tax returns or access the e-Services incentive products and disable the principal consent feature; 2) revise the appeal procedures for *e-file* applicants who fail their suitability check to specify that the Fraud Detection Center has the final approval authority; 3) disable and delete inactive RUP accounts in accordance with IRS procedures or follow the IRS risk-based decision procedures to obtain the required thorough assessment, recommendation, and approval to not implement the required security controls; 4) request the Chief Technology Officer enhance the RUP to require passwords to contain a mix of lower case and upper case letters, set the password length to 12 characters, and prevent the use of Social Security Numbers as usernames and obtain the required thorough assessment, recommendation, and approval to deviate from the IRS password expiration and history requirements; and 5) request the Chief Technology Officer implement a control to allow users to answer a series of challenge questions to unlock their accounts.

We also recommended the Chief Technology Officer enhance the *e-file* application on the Third Party Data Store to post the complete results of the tax compliance check that is performed for an

---

<sup>4</sup> During our fieldwork, the IRS changed its requirement for removing inactive accounts to 180 days.

<sup>5</sup> Office of Management and Budget memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (M-07-16, dated May 22, 2007).



## *Additional Security Is Needed for Access to the Registered User Portal*

---

applicant's spouse and instruct the Cybersecurity office to develop a process to analyze the activities of RUP users and begin reviewing the audit logs.

### *Response*

IRS management agreed to 1) perform suitability checks on delegated users who *e-file* tax returns or access the e-Services incentive products; 2) strengthen the procedures for evaluating *e-file* applicants who fail their suitability check and establish an Executive Review Board to formally consider deviations from the Criminal Investigation Division's recommendations; 3) request the Modernization and Information Technology Services organization enhance the Third Party Data Store to post the entire results from the Automated Suitability Analysis Program; 4) complete a full risk-based decision process and execute a revised risk-based decision memorandum that complies with the Modernization and Information Technology Services organization's standards; 5) prevent the use of Social Security Numbers as usernames, require passwords to contain a mixture of uppercase and lowercase letters, and work with the Modernization and Information Technology Services organization's Cybersecurity office to obtain the requisite thorough assessment, recommendation, and approval to deviate from the IRS' password expiration requirement; and 6) request the Modernization and Information Technology Services organization make programming changes to the RUP to allow users to answer a series of challenge questions to unlock their accounts. The IRS also stated that the RUP audit logs are now being reviewed to detect unauthorized activities.

In addition, the IRS stated it does not believe the final authority for approvals of applicants with criminal records should rest solely with the Criminal Investigation Division, and it revised its procedures, as of July 31, 2009, to lower the minimum password length to eight characters for all systems except the Windows operating system.

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

### *Office of Audit Comment*

We concur with the IRS decision to establish an Executive Review Board to formally consider deviations from the Criminal Investigation Division's recommendations. The IRS stated the new board will include members from the Office of Professional Responsibility along with representatives from other IRS business operating divisions. Members from outside of the Wage and Investment Division should ensure an impartial suitability decision process. Regarding the IRS disagreement with our recommendation to set the password length to 12 characters, we confirmed the IRS lowered its password complexity requirements to require only 8 characters for all non-Windows operating systems. Therefore, we concur with the IRS decision to not set the password length to 12 characters.



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

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 Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

*Table of Contents*

**Background** ..... Page 1

**Results of Review** ..... Page 4

    Some Access Controls for the Registered User Portal  
    and E-Services Applications Were Implemented but  
    Improvements Are Needed ..... Page 4

Recommendations 1 and 2: ..... Page 11

Recommendations 3 through 5: ..... Page 12

Recommendation 6: ..... Page 13

    Audit Logs for the Registered User Portal Are Not Reviewed ..... Page 13

Recommendation 7: ..... Page 15

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology ..... Page 16

    Appendix II – Major Contributors to This Report ..... Page 18

    Appendix III – Report Distribution List ..... Page 19

    Appendix IV – List of Internal Revenue Service  
    E-Services Products ..... Page 20

    Appendix V - Management’s Response to the Draft Report ..... Page 22



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

*Abbreviations*

DAA	Designated Approving Authority
<i>e-file</i>	Electronically file; electronic filing
ETARC	Electronic Tax Administration and Refundable Credits
FDC	Fraud Detection Center
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services
RUP	Registered User Portal
TIN	Taxpayer Identification Number



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

## *Background*

The use of the Internet is an integral part of the Internal Revenue Service's (IRS) mission to deliver top quality service to all taxpayers. The need to use the Internet is partly driven by the IRS Restructuring and Reform Act of 1998,<sup>1</sup> which required the IRS to become more efficient, make tax filing easier, and receive 80 percent of all tax returns electronically by 2007.

To help accomplish this mission, the IRS developed the Registered User Portal (RUP) and e-Services suite of applications. The RUP serves as the entry point for web access to e-Services applications. The e-Services was one of the first business systems modernization projects initiated by the IRS and includes a suite of web-based products<sup>2</sup> that allow tax professionals to submit and retrieve tax-related information and electronically file (*e-file*) tax returns. Tax professionals that *e-file* at least five tax returns per year are also granted access to e-Services incentive products that allow tax professionals to electronically submit a Power of Attorney document to the IRS, send and receive inquiries about individual or business account problems, and download taxpayers' personal tax data to computers outside of the IRS.

***The RUP and e-Services allow tax professionals to use the Internet to e-file tax returns and submit and retrieve tax-related information.***

During the 2008 Filing Season,<sup>3</sup> 58 percent of all tax returns, nearly 90 million of the 155 million tax returns filed, were received electronically. Along with the increased efficiency and other benefits, the RUP and e-Services present security risks. Taxpayers entrust the IRS with their sensitive financial and personal data and expect the IRS to protect these data from unauthorized disclosure and identity theft.

A previous review<sup>4</sup> conducted by the Treasury Inspector General for Tax Administration on tax preparers identified fraudulent activity within the tax preparer environment, which increases our concern of the security risks affecting the RUP and e-Services. We reported that the IRS was not aware of 160 tax preparers who had been assessed tax penalties, were permanently enjoined by a Federal Court, or had been sentenced for abusive tax shelter activities that caused loss to the Federal Government of approximately \$34.9 million. These preparers were still eligible to

---

<sup>1</sup> Pub. L. 105-206, 122 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

<sup>2</sup> See Appendix IV for a list of e-Services products.

<sup>3</sup> The period from January through mid-April when most individual income tax returns are filed.

<sup>4</sup> *Tax Practitioners Promoting Abusive Tax Shelters Are Still Able to Represent Taxpayers Before the Internal Revenue Service* (Reference Number 2009-10-039, dated February 20, 2009).



---

## *Additional Security Is Needed for Access to the Registered User Portal*

---

represent 9,766 taxpayers before the IRS. In addition, the Treasury Inspector General for Tax Administration Office of Investigations has investigated numerous ongoing fraudulent activities in the tax preparation industry. Examples include preparers who overstate their qualifications, steal clients' tax payments or tax refunds, impersonate IRS employees, and misuse the IRS seal or logo. The IRS is especially vulnerable since it does not know how many paid preparers exist and cannot determine the full extent of noncompliance among preparers.

The IRS uses access controls to protect taxpayers' data processed through the RUP. Access controls include authentication, authorization, and accountability. Authentication includes determining who can log on to a system. Authorization determines what a user can do after they are authenticated, and accountability identifies what a user did when they were on the system. Poor access controls could result in intruders gaining unauthorized access to taxpayer data.

The responsibility for managing the RUP and e-Services is shared by the Wage and Investment Division and Modernization and Information Technology Services (MITS) organization.

- The Wage and Investment Division's Electronic Tax Administration and Refundable Credits (ETARC) office sets the policies for the RUP and manages the relationships with key internal and external stakeholders as well as industry partners to increase the IRS' electronic interaction with the public.
- The Wage and Investment Division Electronic Products and Services Support function provides program management for e-Services, including the e-help desk.
- The MITS organization's Portal Program Management office provides program direction, oversight, and central control of the IRS portal environment, including oversight of the contractor that manages the RUP components located in Chicago, Illinois, and Sterling, Virginia.
- The MITS organization's Cybersecurity office administers the Enterprise Directory and Authentication Services, which provides identification and authorization for registered users on the RUP.

All tax professionals who use the e-Services products must register by logging on to the RUP and creating an electronic account. The registration process is a one-time automated process where the user selects a username, password, and personal identification number.

This review was performed at the Wage and Investment Division's ETARC office in Washington, D.C.; the Electronic Products and Services Support function in Andover, Massachusetts; the MITS organization's Portal Program Management office and Enterprise Operations office in New Carrollton, Maryland; and the Cybersecurity office in Martinsburg, West Virginia. We performed the review during the period April through October 2009 and conducted our work 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



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

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.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

## *Results of Review*

### ***Some Access Controls for the Registered User Portal and E-Services Applications Were Implemented but Improvements Are Needed***

The IRS has established some of the access controls that are necessary to protect taxpayer data processed by the RUP and e-Services. Specifically:

- Individuals, businesses, and organizations are required to register on the e-Services web site. The information gathered during this registration process is used to confirm the user's identity.
- Users are automatically locked out after three unsuccessful logon attempts. This control prevents hackers from forcing their way into the system by repeatedly trying to guess a user's password.
- Passwords are masked when typed to strengthen security over passwords.
- E-Service applications display a warning banner to advise all persons attempting to gain access that the system and its information are for authorized users only and attempts to illegally log on to the system could lead to criminal prosecution.
- No group, temporary, or emergency accounts on the RUP identification and authorization servers existed. Avoiding these accounts is important because they offer unauthorized users additional opportunities to access and exploit the system.

Although the IRS has implemented some of the required security controls, additional controls are needed to protect taxpayer information.

### ***Suitability checks were not performed on all users who e-file tax returns and access taxpayer data***

The IRS performs a suitability check when a principal or responsible official of a tax firm applies to file tax returns electronically. The suitability check was originally implemented because electronic filing firms could change tax return data after the taxpayer signed the return but before transmitting the return to the IRS. The ability to alter tax return data without the taxpayer's knowledge increased the risk of fraud for electronic filing firms as opposed to paper tax return preparers. Therefore, the IRS designed the suitability check to screen and monitor *e-file* applicants to ensure they meet and maintain the highest ethical standards.

The suitability check includes a tax compliance check, a check for prior noncompliance with *e-file* requirements, and a criminal background check. The criminal background check is



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

performed on a sample<sup>5</sup> of the applicants. The need to perform these suitability checks increased after the IRS developed the three e-Services incentive products. A tax professional automatically gains access to these incentive products after filing five returns electronically. Despite these risks, the IRS does not perform suitability checks on all users with the ability to *e-file* tax returns and access the e-Services incentive products.

The IRS allows principals and responsible officials to delegate their access rights to employees, partners, members of the firm, or any person with a business relationship with the firm. These “delegated” users are not required to undergo a suitability check. In addition, a principal or responsible official can assign a special “Principal Consent” privilege to a delegated user which allows the delegated user to propagate his or her privileges to other individuals. We found that the IRS had 9,988 delegated users with the ability to *e-file* income tax returns and approximately 6,500 of these users also had access to the e-Services incentive products.

The IRS made a decision to allow principals and responsible officials to assume the risks of delegating their access rights to other individuals and believes the risks are mitigated by requiring principals and responsible officials to file a Power of Attorney<sup>6</sup> with the IRS. However, taxpayers expect the IRS to protect their personal data, and we believe the Power of Attorney document does not provide the same assurance as the suitability check.

Further, since a delegated user does not need to be an employee or member of the firm, any individual can become a delegated user. Many of the delegated users may have questionable backgrounds. For example, in the sample of 111 RUP users that we evaluated, the IRS conducted a criminal background check on 18 users and found 6 had criminal records. A delegated user could steal taxpayer data for identity theft purposes and grant access to other unscrupulous individuals. Reviewing an individual’s background allows the IRS to make the appropriate decision on who should *e-file* tax returns or have access to the RUP and e-Services applications.

In July 2009, the MITRE Corporation<sup>7</sup> completed a review of the processes associated with the IRS *e-file* program and recommended the IRS require all *e-file* applicants, including delegated users, undergo a suitability check. In its response, the IRS stated it would conduct an impact analysis and consider performing eligibility and qualification checks on every individual within a firm, rather than on the firm itself, and possibly assigning a separate Electronic Filing

---

<sup>5</sup> The IRS began conducting criminal background checks on most *e-file* applicants in June 2009.

<sup>6</sup> A Power of Attorney is a written authorization to act on someone else’s behalf in a legal or business matter.

<sup>7</sup> The MITRE Corporation is a not-for-profit organization chartered to work in the public interest. The MITRE Corporation provides expertise in systems engineering, information technology, operational concepts, and enterprise modernization.



*Additional Security Is Needed for  
Access to the Registered User Portal*

Identification Number<sup>8</sup> to specific individuals. We concur with the MITRE Corporation's recommendation and the IRS' proposed corrective action. Assigning a separate Electronic Filing Identification Number to each individual would allow for better accountability and identification of persons accessing e-Services products. However, the IRS has not established a time period for completing its impact analysis.

**Procedures for approving e-file applicants who have a criminal record were not always followed**

The criminal background check is part of the suitability check and includes collecting fingerprint cards and sending the cards to the Federal Bureau of Investigations. If the applicant has a criminal record, the Electronic Products and Services Support function in the Andover Campus<sup>9</sup> submits a Fraud Referral Sheet to the Criminal Investigation Division's Fraud Detection Center (FDC). The FDC reviews the case and makes a recommendation whether to allow the applicant to participate in the e-file program. The applicant may submit an appeal if their application is denied. The FDC will review the appeal and decide whether to approve the application or uphold its previous recommendation. The applicant may submit a second appeal if the FDC upholds its previous recommendation. The second appeal must be sent directly to the Office of Appeals, which reviews the case and makes a recommendation on whether to accept the applicant. IRS procedures do not specify a role for the ETARC office in the appeals process.



We found the appeals procedures are not always followed. \*\*\*\*\*1\*\*\*\*\*

\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*

<sup>8</sup> The IRS requires that participants in the e-file Program use unique numbers called Electronic Filing Identification Numbers to identify who transmitted electronic returns through e-file and their role on the system. The Electronic Filing Identification Number is a six-digit number assigned by the IRS, and one number is assigned to a business entity at an address.

<sup>9</sup> The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.



*Additional Security Is Needed for  
Access to the Registered User Portal*

\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*. The ETARC office believes that, as the business owner of the *e-file* program, it has this authority. We believe the FDC office has more expertise in preventing fraud, and this office’s recommendation should be accepted.

The risk of granting unscrupulous individuals access to the RUP and e-Services significantly increases when the IRS does not follow its procedures for approving users. \*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*1\*\*\*\*\*  
\*\*\*\*\*

**Manual suitability checks on an applicant’s spouse should be automated**

IRS procedures require a tax compliance check on an *e-file* applicant and his or her spouse. For this requirement, the IRS has automated the tax compliance check. The tax information is extracted and analyzed efficiently using the Automated Suitability Analysis Program. This Program uses information from the IRS Master File<sup>10</sup> to determine an applicant’s and his or her spouse’s tax compliance for the last 6 years. The tax compliance information for the applicant is posted to the Third Party Data Store.<sup>11</sup> However, limitations in the Third Party Data Store prevent it from recording the complete results of the spouse’s tax compliance check. As a result, the IRS must perform the spouse’s tax compliance check manually. Although the manual suitability processes are thorough, the processes are labor intensive, inefficient, and increase the risk of human error.

In our sample of 111 e-Services users, 30 users had spouses who required a manual suitability check. The employees in the Electronic Products and Services Support function must use other IRS computer systems to analyze the spouses’ tax compliance data and make a pass or fail decision. Since the employees do not maintain most of the documentation involved in this manual tax compliance check, we could not determine whether all of the required steps were taken.

We believe that enhancing the Third Party Data Store to post the results of a spouse’s tax compliance would reduce the risk of human error, ensure the check is completed in a more timely manner, and allow the IRS to use its staff more efficiently by eliminating the current labor intensive process.

<sup>10</sup> The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

<sup>11</sup> The system used to record and monitor information about individuals who have applied to participate in *e-file*.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

**Inactive user accounts on the RUP were not disabled and deleted in accordance with IRS security policies and procedures**

IRS security policies and procedures require inactive user access accounts to be regularly monitored to ensure unneeded accounts are timely disabled and deleted. Inactive user accounts should be disabled after 45 days and permanently removed after 60 days.<sup>12</sup> The intent is to reduce the opportunity for malicious individuals to gain unauthorized access with an unused access account. The IRS had a total of 380,770 RUP user accounts, as of June 15, 2009, which consisted of the following segments.

- 235,290 registered user accounts. These users have completed the registration process on the RUP and have access to the e-Services products. We found 206,032 (88 percent) of the 235,290 registered users had not accessed their account within 45 days. However, the accounts were not disabled. Rather than implement the control to disable the accounts after 45 days, the IRS set the control to 720 days.
- 143,420 new accounts. These users began but did not complete the registration process. These users do not have access to the e-Services products but pose a risk because the applicant, or an individual posing as the applicant, could take steps to complete the registration process.
- 2,060 locked-out accounts. These are accounts that are locked for various reasons such as inactivity.

We believe many of the above accounts are not needed and should be removed from the RUP after a designated time period. For example, we found 86,553 (37 percent) of the registered user accounts had not been accessed within 720 days.

The IRS did not implement the inactive user account security controls because it wanted to accommodate the users, many of whom have only a seasonal need to use the RUP. Most electronic returns are filed during the 4-month filing season, which runs from January through mid-April each year. The IRS did not want to require tax professionals to re-register on the RUP each year. However, we believe the risks associated with operating the RUP and e-Services are increased when these security controls are not implemented.

Also, the procedures for requesting approval to deviate from these security controls were not followed. The IRS has comprehensive procedures that allow a Designated Approving Authority (DAA)<sup>13</sup> to deviate from required security controls. A risk-based decision must be completed and signed by the DAA to permanently omit a security control from the system. In addition, the DAA must complete a thorough risk assessment identifying potential threats to the system and

---

<sup>12</sup> During our fieldwork, the IRS changed its requirement for removing inactive accounts to 180 days.

<sup>13</sup> The Designated Approving Authority is a senior management executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

review any supporting documentation of alternative approaches and recommendations for mitigation. The MITS organization's Cybersecurity office is required to analyze the risk-based decision and supporting documents and issue a recommendation to the DAA, who has the final authority to accept the risk.

After we raised the lack of inactive user account security controls to the attention of the ETARC office during our fieldwork, officials in this office immediately took action to obtain approval for a permanent deviation for the 45-day inactive account requirement. However, the risk-based decision procedures were not followed. A thorough assessment was not conducted by the DAA or the Cybersecurity office. In addition, the risk-based decision memorandum was not signed by the current DAA.

Lastly, the IRS has not taken action to permanently remove inactive RUP accounts or seek approval to deviate from this required security control. Inactive accounts may remain on the RUP indefinitely or until a user requests his or her account be removed.

Weak controls over user accounts could allow unauthorized individuals to gain access to the accounts and access taxpayer's personal information and commit fraudulent activities.

**Password and username controls were not implemented**

The IRS did not implement the required password complexity and username security controls for the RUP. Specifically:

- Passwords are not set to require a mix of lower case and upper case letters.
- Passwords are not set to expire after 60 days as required. Users' passwords are set to expire after 180 days.
- Password minimum length is set to 8 characters instead of the required 12 characters.
- Password histories are not maintained for the last 24 passwords. Currently, only the last five passwords are maintained.
- Users are allowed to use Social Security Numbers as their username. Usernames are used along with a password to identify a system user.

The IRS did not implement the same password and username security controls that it required for its employees because the IRS wanted to make the RUP user friendly and accommodate the tax preparation firms. IRS officials informed us that too many password controls could create an undue burden on tax preparers during filing season, and possibly affect the timely filing of income tax returns.



*Additional Security Is Needed for  
Access to the Registered User Portal*

Specifically on the use of Social Security Numbers as usernames, the Office of Management and Budget<sup>14</sup> required Federal agencies to implement security requirements to explore alternatives to the usage of Social Security Numbers as a personal identifier. Federal agencies were required to develop a plan to eliminate or reduce the unnecessary use of Social Security Numbers by September 2007 and take actions to eliminate or reduce the use of Social Security Numbers by March 2009. In response to the Office of Management and Budget memorandum, the IRS prepared the Social Security Number Elimination and Reduction Implementation Plan, dated November 29, 2007, and stated it is committed to achieving compliance and ultimately reducing risk by eliminating the unnecessary use of Social Security Numbers. However, the ETARC office informed us that e-Services users will continue to be allowed to use their Social Security Number as their username because the IRS has not developed a security policy prohibiting this practice.

The IRS should enforce its security policy and ensure user accounts are protected with strong passwords and usernames that cannot be easily guessed. The existence of weak passwords and the ability to use Social Security Numbers as personal identifiers present security vulnerabilities that could be exploited by a hacker. Usernames on e-Services are at a higher risk for disclosure, since usernames are not masked. Usernames are shown in clear text when typed. In addition, the IRS Helpdesk can provide any person an account username if they correctly answer two challenge questions. External threats for stealing taxpayer data or sabotaging computer systems can be greatly reduced with effective password and username controls.

**The account lockout control was not fully implemented**

The National Institute of Standards and Technology<sup>15</sup> recommends Federal agencies configure systems to automatically lock out a user after three unsuccessful logon attempts. The account lockout duration should be permanent until an authorized system administrator unlocks the user account. For the IRS, the account lockout control is one control to prevent unauthorized access to taxpayer information. However, this control was only partially implemented.

The IRS implemented the security control that automatically locks out users after three unsuccessful logon attempts on the e-Services. \*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\* Due to the large number of registered users on e-Services and the increased workload it may pose on the IRS Helpdesk, \*\*2\*\*  
\*\*\*\*\*2\*\*\*\*\*  
\*\*\*\*\*2\*\*\*\*\*.

<sup>14</sup> Office of Management and Budget memorandum *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (M-07-16, dated May 22, 2007).

<sup>15</sup> The National Institute of Standards and Technology is a Federal technology agency within the Department of Commerce that develops and promotes measurement, standards, and technology.



---

## *Additional Security Is Needed for Access to the Registered User Portal*

---

We believe that, given enough time and potential to try multiple username and password combinations, an attacker might eventually succeed in compromising the security of e-Services and gain access to sensitive taxpayer information.

### **Recommendations**

**Recommendation 1:** To ensure taxpayer information is properly safeguarded and to strengthen security for e-Services, the Director, ETARC, Wage and Investment Division, should require suitability checks on delegated users who *e-file* tax returns or access the e-Services incentive products and disable the principal consent feature on e-Services that allows a user to propagate his or her privileges to other users.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated it would implement suitability checks on delegated users who *e-file* tax returns or access the e-Services incentive products, subject to available funding and the MITS organization's resource prioritization. The IRS also stated this action would eliminate the need to disable the e-Services principal consent feature.

**Office of Audit Comment:** We concur with the IRS statement that implementation of suitability checks on delegated users would eliminate the need to disable the e-Services principal consent feature.

**Recommendation 2:** To ensure only qualified applicants who meet IRS suitability standards are approved for the *e-file* program or given access to the e-Services incentive products, the Director, ETARC, Wage and Investment Division, should stop overturning the FDC's recommendations and revise the appeal procedures for *e-file* applicants and other tax professionals who fail their suitability check. The procedures should specify that the Criminal Investigation Division's FDC has the final authority to approve or disapprove an applicant with a criminal record.

**Management's Response:** The IRS agreed that documentation of IRS final authority to approve or disapprove *e-file* applicant appeals should be strengthened and the criteria by which applicants' appeals are evaluated should be clarified. The IRS stated that it recognized the research and recommendations of the FDC are a vital component of the approval process and believes that consideration should be given to extenuating circumstances, such as the nature of the offence and the length of time since the offence was committed.

In addition, the IRS believes the final authority for approvals of applicants with criminal records should not rest solely with the Criminal Investigation Division, and the IRS recognizes the need to have a comprehensive review of any deviations from the Criminal Investigation Division's recommendations. Therefore, the IRS consulted with Criminal Investigation Division management and agreed that the IRS will establish a



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

cross-business division Executive Review Board to formally consider deviations from the Criminal Investigation Division's recommendations. The new board will include members from the Wage and Investment Division and the Office of Professional Responsibility, along with representatives from other business operating divisions. Further, the IRS will update its procedures to clearly reflect the standards of review and ensure a more consistent, balanced, and impartial suitability decision process.

**Office of Audit Comment:** We concur with the IRS decision to strengthen its procedures for evaluating applicants with criminal records and establish an Executive Review Board to formally consider any deviations from the Criminal Investigation Division's recommendations.

**Recommendation 3:** To reduce the risk of human error and the amount of time needed for manually conducting a tax compliance check for an *e-file* applicant's spouse, the Chief Technology Officer should enhance the *e-file* application on the Third Party Data Store to post the complete results of the Automated Suitability Analysis Program's spouse tax compliance check.

**Management's Response:** The IRS agreed with this recommendation. The Director, ETARC, Wage and Investment Division, will submit a Unified Work Request to the MITS organization to request programming changes to the Third Party Data Store to allow posting of the complete results of the Automated Suitability Analysis Program's spouse tax compliance check.

**Recommendation 4:** To mitigate the risk of an unauthorized intruder accessing an inactive access account, the Director, ETARC, Wage and Investment Division, should disable and delete inactive accounts in accordance with IRS procedures or follow the IRS' risk-based decision procedures to obtain the required thorough assessment, recommendation, and approval from the MITS organization's Cybersecurity office.

**Management's Response:** The IRS agreed with this recommendation and stated it will work with the MITS organization's Cybersecurity office to complete a full risk-based decision process, including the analysis and review, and will execute a revised risk-based decision memorandum that complies with the MITS organization's standards and replaces the current memorandum dated September 29, 2009.

**Recommendation 5:** To make passwords more difficult to guess by unauthorized individuals and to decrease the use of Social Security Numbers as usernames, the Director, ETARC, Wage and Investment Division, should:

- Request the Chief Technology Officer enhance the identification and authorization component of the RUP to require passwords to contain a mix of lower case and upper case letters, set the password length to 12 characters, and prevent the use of Social Security Numbers as usernames.



---

## *Additional Security Is Needed for Access to the Registered User Portal*

---

- Obtain the required thorough assessment, recommendation, and approval from the Cybersecurity office and approval from the DAA to deviate from the IRS password expiration and history requirements.

**Management's Response:** The IRS partially agreed with this recommendation. For the first bullet above, the IRS agreed to prevent the use of Social Security Numbers as usernames and to require passwords to contain a mixture of uppercase and lowercase letters. The IRS disagreed with the recommendation to set the password length to 12 characters, citing its revised procedures, dated July 31, 2009, to lower the minimum password length to 8 characters for all systems except the Windows operating system.

For the second bullet above, the IRS stated that although it took initial action to implement the risk-based decision procedures, it recognizes additional work needs to be conducted. The IRS stated it will work with the MITS organization's Cybersecurity office to obtain the requisite thorough assessment, recommendation, and approval from the DAA to deviate from the IRS password expiration requirement.

The IRS stated it will submit a Unified Work Request to the MITS organization requesting the RUP be brought into compliance with the IRS password composition and history retention requirements. In addition, the IRS will submit a Unified Work Request to prevent Social Security Numbers from being used as usernames. In the interim, the ETARC office will modify an existing Unified Work Request to alert applicants not to use their Social Security Numbers as their usernames.

**Office of Audit Comment:** We confirmed the IRS lowered its password complexity requirements during our audit to require only eight characters for all non-Windows operating systems. Therefore, we concur with the IRS decision to not set the password length to 12 characters.

**Recommendation 6:** To prevent hackers from forcing their way into the RUP, the Director, ETARC, Wage and Investment Division, should request the Chief Technology Officer implement a control to allow users to answer a series of challenge questions to unlock their accounts.

**Management's Response:** The IRS agreed with this recommendation and stated a Unified Work Request will be submitted to the MITS organization requesting programming modifications to include a series of challenge questions to allow users to unlock their accounts. The IRS also stated that other resource issues need to be evaluated to address additional costs associated with implementing this corrective action.

## ***Audit Logs for the Registered User Portal Are Not Reviewed***

The IRS is required to create, protect, retain, and analyze the audit logs of information systems that process taxpayer data to detect unlawful or unauthorized activities. Every interaction with



---

## *Additional Security Is Needed for Access to the Registered User Portal*

---

taxpayer data through a system or application is an auditable event and should be reviewed. Audit logs should be used for periodic reviews and for real-time analysis. We found the RUP audit logs created by the web servers located in Chicago, Illinois, and Sterling, Virginia, capture many of the required auditable events and are synchronized to the required IRS authoritative time source.<sup>16</sup> However, the IRS does not review the audit logs.

The Cybersecurity office provided three reasons why the RUP audit logs are not reviewed.

- 1) The data captured in the RUP audit logs are too voluminous to analyze. The Cybersecurity office informed us it has attempted numerous techniques to reduce the amount of data captured in the logs. However, its attempts to make the audit logs useful were not successful.
- 2) The Cybersecurity office does not have a process in place to review the activities of external users of systems such as the RUP.
- 3) The IRS has not allocated sufficient resources to the Security Audit and Analysis System<sup>17</sup> to review all audit logs from every computer system. Therefore, the IRS prioritizes the systems for which it will analyze audit logs, and the RUP audit logs are not ranked high enough on the priority list.

Proper review of audit logs ensures that activities performed on a system can be traced back to an individual. In addition, inadequate accountability controls could prevent the IRS from identifying and investigating security incidents, policy violations, fraudulent activity, and operational problems. We believe that the lack of RUP audit log reviews increases the likelihood that questionable activities could go unnoticed and intruders could gain access to sensitive taxpayer data without being detected.

---

<sup>16</sup> The IRS requires all servers and audit logs be synchronized to the Greenwich Mean Time, which refers to a high-precision atomic standard to set time.

<sup>17</sup> The Security Audit and Analysis System implements a data warehousing solution to provide online analytical processing of audit log data. The System enables the IRS to detect potential unauthorized accesses to IRS systems. It provides analysis and reporting capabilities for all modernized systems and for some current processing environment applications.



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

***Recommendation***

***Recommendation 7:*** To detect unlawful or unauthorized activities on the RUP, the IRS Chief Technology Officer should instruct the Cybersecurity office to develop a process to analyze the activities of RUP users and begin reviewing the audit logs.

***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the RUP audit logs are currently being reviewed to detect unlawful or unauthorized activities. The IRS is currently using RealSecure to generate events in the audit logs. The employees are also required to document the date of their reviews.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine whether the IRS established effective access and audit trail controls for the RUP, which allows access to the IRS' e-Services<sup>1</sup> suite of applications, to protect taxpayer data from unauthorized disclosure. To accomplish our objective, we:

- I. Determined whether authentication controls were operating effectively to limit access to authorized users.
  - A. Interviewed the Electronic Tax Administration office to determine whether an e-Authentication risk assessment was completed.
  - B. Determined whether users have been properly registered and authorized.
  - C. Determined whether generic, default, or duplicate accounts exist.
  - D. Determined whether group accounts exist that would allow users to perform activities on the system without being identified.
  - E. Determined whether temporary or emergency accounts exist.
  - F. Determined whether inactive accounts exist.
  - G. Determined whether user permissions have been restricted based on the principle of least privilege, which limits users' abilities on the system to only those necessary to complete their assigned tasks.

#### **Sampling Methodology**

The IRS was unable to query the SiteMinder component of the Enterprise Directory and Authentication Services system to determine the total population of RUP users who have access to the e-Services incentive products. Therefore, we worked with the system administrators in the IRS MITS organization's Cybersecurity office to select a random sample and accomplish this audit test. We selected 111 authorized users with access to the 3 e-Services incentive products (Disclosure Authorization, Electronic Account Resolution, and Transcript Delivery System). The users are segmented on the SiteMinder according to the first letter or digit of their username. There are a total of 36 segments on the system – 26 alphabets (A-Z), and 10 numbers (0-9). We

---

<sup>1</sup> See Appendix IV for a list of e-Services products.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

- selected three users in each alphabet and number, except digits 0 and 8. We selected 5 users for the number 0, and 4 users for the number 8. To verify the validity and reliability of the data in the SiteMinder, we compared the total number of RUP users on SiteMinder to the total number of RUP users on the IRS Third Party Data Store, which is a separate system used to record and monitor information about individuals who have applied to participate in the *e-file* program. Total number of users on the Third Party Data Store was commensurate with the total users on the SiteMinder.
- H. Determined whether password control for user accounts meets IRS guidelines.
  - I. Interviewed system administrators to determine whether the system automatically locks out a user after three unsuccessful logon attempts.
  - J. Determined whether the appropriate warning banner is displayed to warn all persons attempting to gain access to the system that the system and its information are for authorized users only and that attempts to illegally log on to the system could lead to criminal prosecution.
- II. Determined whether the IRS properly captured, stored, analyzed, and retained audit trails.
- A. Obtained and reviewed the System Security Plan.
  - B. Determined whether audit trails were properly captured.
  - C. Determined whether audit trails were properly stored.
  - D. Determined whether audit trails were properly retained.
  - E. Determined whether audit trails were properly analyzed to detect unauthorized activities.

### **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 Wage and Investment Division's policies and procedures for processing *e-file* applications and administering RUP users' access accounts, and the MITS organization's processes for capturing and analyzing audit trails. We evaluated these controls by interviewing management, reviewing case files, and analyzing RUP users' accounts.



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

**Appendix II**

*Major Contributors to This Report*

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Allen Gray, Audit Manager  
John Brown, Senior Auditor  
Charles Ekunwe, Senior Auditor  
Cari Fogle, Senior Auditor  
Michelle Griffin, Senior Auditor



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Commissioner for Services and Enforcement SE  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division  
SE:W:ETARC  
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 Liaisons:  
    Commissioner, Wage and Investment Division SE:W  
    Director, Program Oversight OS:CIO:SM:PO



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

## Appendix IV

### *List of Internal Revenue Service E-Services Products*

This appendix presents the different applications within the IRS' e-Service suite of products<sup>1</sup> that can be accessed through the RUP.

1. **Disclosure Authorization**: The Disclosure Authorization application provides the ability for the registered user to edit, sign, and transmit a disclosure authorization transaction.
2. **Electronic Account Resolution**: Electronic Account Resolution allows tax professionals to expedite closure on a client's account problems by electronically sending and receiving account-related inquiries. Tax professionals may inquire about individual or business account problems, refunds, and missing payments. Tax professionals must have a Power of Attorney document on file at the IRS before accessing a client's account.
3. **Transcript Delivery System**: Transcript Delivery System provides self-service for return and account information requests by external tax professionals through the RUP. Transcript Delivery System transactions include self-service electronic communication, where the user can request and receive a transcript of a taxpayer's personal tax data interactively through the RUP.
4. **Registration Services**: Before using other e-Services products, tax professionals must register online on the Registration Services to create an electronic account. The registration process is a one-time process for tax professionals to select a username, password, and personal identification number. An on-screen acknowledgment immediately confirms the registration process. For security purposes, a confirmation code is mailed to the tax professional to complete the registration process.
5. **E-File Application**: IRS *E-File* Application provides the online interface component through which an organization may apply for participation in the IRS *e-file* program. Functionality includes the ability to initially apply and/or revise an existing application for processing by the IRS.
6. **Preparer Tax Identification Number Application**: The Preparer Tax Identification Number Application lets paid preparers apply for and receive a personal identification number immediately over the Internet.

---

<sup>1</sup> The first three e-Services products listed are referred to as incentive products.



*Additional Security Is Needed for  
Access to the Registered User Portal*

---

7. **Interactive Taxpayer Identification Number (TIN) Matching**: Interactive TIN Matching is a prefilling service offered to banks or others that pay income subject to backup withholding. Authorized payers can match up to 25 TIN and name combinations against IRS records before submitting an information return. This prefilling check prevents mismatches and possible penalties for the payer.
8. **Bulk TIN Matching**: Similar to Interactive TIN Matching, the Bulk TIN Matching allows authorized users to match up to 100,000 TIN and name combinations with IRS records prior to submission.



COMMISSIONER  
WAGE AND INVESTMENT DIVISION

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
ATLANTA, GA 30308

MAR 26 2010

RECEIVED  
MAR 26 2010  
BY: JAF

MEMORANDUM FOR MICHAEL R. PHILLIPS  
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard Byrd, Jr. *Richard Byrd*  
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report - Additional Security Is Needed for Access to  
the Registered User Portal (Audit #200920014)

Thank you for the opportunity to comment on the draft audit report concerning access to the IRS' Registered User Portal (RUP). In brief, you have made a number of valuable recommendations with which we generally agree and will implement, subject to resources limitations. Some of the issues identified in your report can be addressed through improved documentation of policies and procedures and we are already taking steps to put these measures in place.

Protecting taxpayer data from unauthorized disclosure is critical to the successful administration of the tax system. We are committed to active program management to ensure the IRS is prepared to address evolving security risks. Your review identified several areas where procedures were not followed or documented fully. We are working to correct these issues.



t. While we agree the process for making suitability determinations and the criteria for evaluating appeals should be more completely documented, we do not agree with your recommendation that the CID recommendation be the final determinant of the suitability process. Instead, departures from CID's position should be carefully evaluated, and should be considered and approved by a cross-divisional executive board. We believe consideration of other factors beyond the applicant's criminal history, such as the nature of the offence involved and the length of time since the offence occurred, results in better and fairer e-file applicant suitability decisions.

In response to your concerns, we will implement new controls, including a clearly documented set of criteria to be used in evaluating cases where there is any



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

2

consideration to depart from the initial CI recommendation, and establishment of an Executive Review Board composed of members from functions both within and outside Wage and Investment to consider any changes. Further, IRS will ensure relevant Internal Revenue Manuals are updated accordingly.

I want to stress our commitment to a strong e-File program. Given that more than two-thirds of taxpayers e-Filed last year, and an e-File mandate will take effect in 2011, IRS is very focused on ensuring the integrity and safety of the program. For this reason, we will ensure a thorough and timely review process occurs before any applicant who does not pass CI's background screening is granted admission.

Your report references discrepancies with the Risk Based Decision (RBD) procedures. While we have made some progress toward completing the RBD process, we recognized additional work is needed and our ETARC organization will work with MITS Cybersecurity to properly conduct the analysis and review needed to execute a revised RBD memo that meets the standards you recommend.

In summary, we are committed to making the RUP as secure and useful as possible for taxpayers and tax professionals. Attached are our specific comments to your recommendations. If you have any questions, please contact me, or members of your staff may contact David Williams, Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, at (202) 622-7990.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

Attachment

**RECOMMENDATION 1:** To ensure taxpayer information is properly safeguarded and to strengthen security for e-Services, the Director, ETARC, should require suitability checks on delegated users who e-file tax returns or access the e-Services incentive products and disable the principal consent feature on e-Services that allows a user to propagate his or her privileges to other users.

**CORRECTIVE ACTION**

The IRS agrees with the recommendation to require suitability checks on delegated users who e-file tax returns or access the e-Services incentive products. The IRS will take the necessary actions to implement suitability checks on delegated users who e-file tax returns or access the e-Services incentive products, subject to available funding and Modernization and Information Technology Services (MITS) resource prioritization. Implementation of suitability checks on delegated users will, consequently, eliminate the need to disable the e-Services principal consent feature.

**IMPLEMENTATION DATE**

June 15, 2011

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.

**RECOMMENDATION 2:** To ensure only qualified applicants who meet IRS suitability standards are approved for the e-file program or given access to the e-Services incentive products, the Director, ETARC, should stop overturning the FDC's recommendations and revise the appeal procedures for e-file applicants and other tax professionals who fail their suitability check. The procedures should specify that the Criminal Investigation Division's FDC has the final authority to approve or disapprove an applicant with a criminal record.

**CORRECTIVE ACTION**

The IRS agrees that documentation of IRS final authority to approve or disapprove e-file applicant appeals should be strengthened and the criteria by which applicants' appeals are evaluated should be more clearly delineated. While recognizing that the research and resulting recommendations of the Fraud Detection Center is a vital component of the approval process, it is believed that consideration should be given, when appropriate, to extenuating circumstances, such as the nature of the offence and the length of time that has elapsed since the offence was committed.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

2

We believe final authority for approvals of applicants with criminal records should not rest solely with the Criminal Investigation Division (CID). But we recognize the need to have a comprehensive review of any deviations from their recommendations. Therefore, we have consulted with CID management and have agreed that IRS will establish a cross-business division Executive Review Board to formally consider any deviations from CID recommendations. That board will include members from the Wage and Investment (W&I) Division and the Office of Professional Responsibility, along with representatives from other Business Operating Divisions. Furthermore, the relevant Internal Revenue Manuals (IRMs) will be updated to clearly reflect the standards of review and ensure a more consistent, balanced, and impartial suitability decision process.

**IMPLEMENTATION DATE**

November 15, 2010

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.

**RECOMMENDATION 3:** To reduce the risk of human error and the amount of time needed for manually conducting a tax compliance check for an *e-file* applicant's spouse, the Chief Technology Officer should enhance the *e-file* application on the Third Party Data Store to post the complete results of the Automated Suitability Analysis Program's spouse tax compliance check.

**CORRECTIVE ACTION**

The IRS agrees with this recommendation. The IRS checks the tax compliance of the associated primary or secondary Social Security Numbers (SSNs) of the jointly-filed returns of *e-file* principals and responsible officials. An *e-file* applicant's spouse would only be checked for joint tax compliance and does not go through any other suitability check since they are not listed in any roles on the *e-file* application and not subject to participation rules.

The Director, Electronic Tax Administration and Refundable Credits (ETARC), will submit a Unified Work Request (UWR) by January 15, 2011, to request the requisite programming changes to the Third Party Data Store so that complete results of the Automated Suitability Analysis Program's spouse tax compliance check are posted. Since the requested action will be subject to funding and resource prioritization by MITS, submission of the UWR will complete the corrective action.



*Additional Security Is Needed for  
Access to the Registered User Portal*

3

**IMPLEMENTATION DATE**

January 15, 2011

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.

**RECOMMENDATION 4:** To mitigate the risk of an unauthorized intruder accessing an inactive access account, the Director, ETARC, should disable and delete inactive accounts in accordance with IRS procedures or follow the IRS' risk-based decision procedures to obtain the required thorough assessment, recommendation, and approval from the MITS Cybersecurity office.

**CORRECTIVE ACTION**

IRS agrees with this recommendation. Rather than disabling or deleting inactive accounts, ETARC will work with MITS Cybersecurity to complete a full risk-based decision process – including the analysis and review – and will execute a revised Risk Based Decision (RBD) memo that complies with MITS standards and replaces the current memorandum executed September 29, 2009.

**IMPLEMENTATION DATE**

December 15, 2010

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration & Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.

**RECOMMENDATION 5:** To make passwords more difficult to guess by unauthorized individuals and to decrease the use of Social Security Numbers as usernames, the Director, ETARC, should:

- Request the Chief Technology Officer enhance the identification and authorization component of the RUP to require passwords to contain a mix of lower case and upper case letters, set the password length to 12 characters, and prevent the use of Social Security Numbers as usernames.



---

*Additional Security Is Needed for  
Access to the Registered User Portal*

---

4

- Obtain the required thorough assessment, recommendation, and approval from the Cybersecurity office and approval from the DAA to deviate from the IRS password expiration and history requirements.

**CORRECTIVE ACTION**

With regard to the first bullet, IRS agrees with two of the three components of this recommendation. We agree to prevent the use of SSNs as usernames and to require passwords to contain a mix of lower case and upper case letters. We disagree with the recommendation to increase the password length to 12 characters. Internal Revenue Manual 10.8.1, Information Technology (IT) Security, Policy and Guidance, revised July 31, 2009, establishes a required minimum password length of eight characters for all systems except Windows OS. Therefore, the Registered User Portal (RUP) remains in compliance with the minimum password length requirement.

With regard to the second bullet, we believe, for the purpose of promoting and encouraging RUP use by outside stakeholders, the 90-day password expiration requirement is too restrictive. Although we took initial action, based on TIGTA's recommendation to implement the RBD procedures, we recognize additional work needs to be done. To that end we will work with MITS Cybersecurity to obtain the requisite thorough assessment, recommendation, and approval from the Designated Approving Authority to deviate from the IRS password expiration requirement.

We will submit a UWR by January 15, 2011, to bring the RUP into compliance with IRM 10.8.1.5.10 regarding password composition and history retention. We will also submit a UWR by January 15, 2011 to prevent the SSNs from being used as usernames. In the interim, ETARC will modify an existing UWR to alert applicants not to use their SSNs as their usernames. Since the requested actions will be subject to funding and resource prioritization by MITS, submission of the UWRs will complete the corrective action.

**IMPLEMENTATION DATE**

January 15, 2011

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration & Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.



*Additional Security Is Needed for  
Access to the Registered User Portal*

5

**RECOMMENDATION 6:** To prevent hackers from forcing their way into the RUP, the Director, ETARC, should request the Chief Technology Officer to implement a control to allow users to answer a series of challenge questions to unlock their accounts.

**CORRECTIVE ACTION**

The IRS agrees with this recommendation. We will submit a UWR by January 15, 2011, requesting programming modifications to include a series of challenge questions to unlock user accounts. Since the requested action will be subject to funding and resource prioritization by MITS, submission of the UWR will complete the corrective action. Furthermore, other resource issues need to be evaluated to address additional costs (staff phones and/or enhancement to the application) associated with implementing this corrective action.

**IMPLEMENTATION DATE**

January 15, 2011

**RESPONSIBLE OFFICIAL**

Director, Electronic Tax Administration & Refundable Credits, Wage and Investment Division

**CORRECTIVE ACTION MONITORING PLAN**

We will monitor this corrective action as part of our internal management control process.

**RECOMMENDATION 7:** To detect unlawful or unauthorized activities on the RUP, the IRS Chief Technology Officer should instruct the Cybersecurity office to develop a process to analyze the activities of RUP users and begin reviewing the audit logs.

**CORRECTIVE ACTION**

The RUP logs are now being reviewed to detect unlawful or unauthorized activities. We are using RealSecure to generate events in the monitored logs. The specialists are also required to document the date of their reviews.

**IMPLEMENTATION DATE**

N/A

**RESPONSIBLE OFFICIAL**

N/A

**CORRECTIVE ACTION MONITORING PLAN**

N/A