TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Security Controls Over Electronic Crimes Labs Need Improvement

December 21, 2020

Reference Number: 2021-20-003

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Security Controls Over Electronic Crimes Labs Need Improvement

Final Audit Report issued on December 21, 2020
Reference Number 2021-20-003

Why TIGTA Did This Audit

This audit was initiated to determine whether IRS Criminal Investigation is implementing effective security controls over digital evidence and the Electronic Crimes labs.

Criminal Investigation serves the public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes. There are 60 Electronic Crimes labs nationwide where computer investigative specialists support special agents in collecting and analyzing digital evidence.

Impact on Taxpayers

Electronic Crimes computer investigative specialists and special agents collect and analyze digital evidence to prosecute criminal cases. According to the IRS, in Fiscal Year 2019, the Electronic Crimes labs supported special agents on 477 operations and collected and analyzed more than 1,400 terabytes of data for evidence. Without proper logical, physical, and environmental controls over the Electronic Crimes labs, there is an increased risk that digital evidence could be compromised and negatively affect public trust in the IRS.

What TIGTA Found

The Electronic Crimes section within the Technology Operations and Investigative Services unit in Criminal Investigation [redacted]

The Facilities Management and Security Services organization is responsible for implementing and evaluating IRS physical security. [redacted]

What TIGTA Recommended

[redacted]

The IRS agreed with all the recommendations. The IRS plans to identify and implement Internal Revenue Manual security controls for [redacted] and document any exceptions, conduct a quarterly reconciliation of [redacted], and identify an alternate storage site to store backup copies of original digital evidence or develop a risk-based decision if off-site backup is not feasible. The IRS also stated that it issued an e-mail to ensure that physical security specialists include Criminal Investigation assigned space as part of physical security inspections.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

December 21, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

M. Weir for

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Controls Over Electronic Crimes Labs Need Improvement (Audit # 202020020)

This report presents the results of our review to determine whether Internal Revenue Service (IRS) Criminal Investigation is implementing effective security controls over digital evidence and the Electronic Crimes labs. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

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

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 Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

Internal Revenue Service (IRS) Criminal Investigation (CI) serves the public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes. The Technology Operations and Investigative Services unit in CI operates and maintains the IRS CI computer network,[1] evaluates the technical aspects of network software and hardware, and recovers and analyzes investigative digital evidence. The Electronic Crimes (E-Crimes) section is part of the Technology Operations and Investigative Services unit and employs computer investigative specialists (CIS) who support special agents in collecting and analyzing digital evidence.

CISs are trained in the acquisition, handling, and analysis of digital evidence. They assist special agents by securing taxpayer data, eliminating information of nonevidentiary value, and performing analysis to extract critical information. According to the IRS, in Fiscal Year 2019, CISs assisted special agents on 477 search warrant operations, for which they collected and analyzed more than 1,400 terabytes of data. As of June 2020, CISs assisted with more than 600 operations and collected more than 800 terabytes of data for Fiscal Year 2020.

E-Crimes has 60 labs nationwide in eight designated regional areas.[2] CISs are assigned to 47 of the labs. In December 2019, the E-Crimes section proposed a consolidation that would reduce the number of lab locations from 60 to 18. The E-Crimes section plans to reduce the number of smaller labs through attrition by not backfilling vacant CIS positions in remote locations, with the goal of reducing overhead, space, and utility costs. An E-Crimes official stated that this consolidation would likely take at least five years to complete.

[redacted],[3] [redacted]

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

[2] E-Crimes offices span 61 locations including headquarters in Woodbridge, Virginia, that does not contain a lab.

[3] Treasury Inspector General for Tax Administration, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

Results of Review

****************************2**************************

The CISs analyze digital evidence used to prosecute cases in court. To perform digital evidence analysis, IRS personnel stated that the CISs use high-powered [redacted] that do not connect to the IRS network or the Internet. We found that the E-Crimes section did not adhere to agency information system policy to manage and secure its [redacted].

The Internal Revenue Manual (IRM)[4] provides detailed policies for the management and security of information systems within the IRS. Specifically, the IRM provides guidance on all aspects of security for the protection of information technology resources. [redacted][5]

[redacted]

*********************************2*******************************
2

[redacted]

[4] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (May 19, 2019).

[5] Pub. L. No. 116-25 133 Stat. 981.

[6] Six of the 28 [redacted] we tested were inoperable, so we could not test the security controls. However, we included those [redacted] in our inventory testing.

***************2****************

[redacted]

[redacted]

***************2****************

[redacted]

***************2****************

[redacted]

***************2****************

[redacted]

[redacted]

Recommendation 1: [redacted]

Management's Response: The IRS agreed with this recommendation. [redacted]

The Hardware Inventory of ******2******* Workstations Is Inaccurate

We reviewed two hardware inventories for [redacted] assets dated June 4, 2020, and July 6, 2020, respectively.[7] The inventories included information such as the asset's brand, model, barcode number, serial number, user, contact name, location, and last verified date and time. Based on the information to be captured in the inventory, CI should have sufficient information to track and report assets accurately. However, we found that both inventories we reviewed were inaccurate.

During site visits, we observed [redacted]. To assess the accuracy of the June 4, 2020, inventory, we compared the [redacted] barcode, location, and user assigned to the hardware inventory. We found that [redacted] (86 percent) of the [redacted] were accurately accounted for, including the correct barcode, location, and user assigned in the inventory. However, [redacted] (14 percent) of the [redacted] were missing from the inventory. We requested another inventory dated July 6, 2020, and found no changes from the June 4, 2020, inventory.

At one [redacted], we found one [redacted] without an IRS barcode number. The CIS e-mailed us the barcode information after the site visit. We compared the barcode information provided to the inventory dated June 4, 2020, and found that the location and user information did not match the [redacted] observed during the site visit. We also tried to verify the [redacted] serial number and found no corresponding asset. The [redacted] information provided was also not located in the July 6, 2020, inventory. We notified CI personnel, and they confirmed that the [redacted] from that [redacted] was not recorded in the hardware inventory.

The IRM requires the development and documentation of an inventory of information system components that accurately reflects current information systems with sufficient detail for tracking and reporting. Computer operations administrators are responsible for maintaining CI's inventory. We met with computer operations administrators who stated that they send out monthly e-mails to the CISs to verify the accuracy of the [redacted] inventory. The computer operations administrators further stated that they did not believe that the CISs were required to verify their inventory of [redacted] and did not follow up if they did not receive verification of a the CISs' inventory. However, the Hardware and Software Inventory and Distribution Policy and Procedures dated June 2020 requires computer operations

[7] Hardware inventory is maintained in the Knowledge, Incident/Problem, Service Asset Management database, which is the asset management tool used to track information technology and non–information technology equipment.

administrators to e-mail an extract of the information technology inventory monthly to the CIS.[8] The Hardware and Software Inventory and Distribution Policy and Procedures states the inventory list must be verified for accuracy and CIS e-mail verification is required. One computer operations administrator stated that he or she was unaware that the current policy required CIS verification of the inventory. Inaccurate inventory impedes the ability to timely detect lost or stolen [redacted].

Recommendation 2: The Chief, CI, should ensure that the hardware inventory requirements are clearly communicated and the inventory is updated as required.

> **Management's Response:** The IRS agreed with this recommendation. The IRS Asset Management Project Office dictates the Service-wide policy for asset inventories. The inventory plan requires an annual inventory, and the Government Accountability Office subsequently performs an annual audit. In order to assure that the required annual inventories are updated as required, both the User Support and the E-Crimes Standard Operating Procedures will be updated and an inventory touchpoint between the two sections will occur on a quarterly basis. These updated Standard Operating Procedures will be communicated to both the User Support and E-Crimes/Digital Forensics organizations.

*******************2********************

In April 2008, we reported[9] that the CISs were not safeguarding a backup copy of the original evidence at a secure, off-site location. At the time, the E-Crimes section stated that it was preparing to implement an information technology solution that would provide for dual location storage of digital evidence within a few years. For each of the [redacted] E-Crimes labs we visited during this audit, we found [redacted]

The IRM requires an alternate storage site, including the necessary agreements to permit the storage and retrieval of information system backup information. The alternate site shall be separate from the primary storage site and shall not be susceptible to the same threat as the primary location. In addition, the alternate site must provide information security safeguards equivalent to that of the primary site.

[redacted] The E-Crimes Standard Operating Procedures dated May 25, 2019,[10] require the CISs to

[8] CI, *Computer Operations Administrator Standard Operating Procedures, Hardware and Software Inventory and Distribution Policy and Procedures* (June 2020).

[9] Treasury Inspector General for Tax Administration, Ref. No. 2008-10-106, *While Renowned for Its Forensic Capabilities, the Digital Evidence Program Faces Challenges and Needs More Controls* (Apr. 2008).

[10] IRS CI, *Electronic Crimes Standard Operating Procedures* (May 25, 2019).

maintain a backup copy of original images on separate media for redundancy purposes. However, there is no requirement for these backup copies to be stored at an alternate, off-site location for contingency purposes. [redacted]

Recommendation 3: [redacted]

Management's Response: The IRS agreed with this recommendation. [redacted]

Physical Security and Environmental Controls Are Inadequate

We tested six physical security and environmental controls at [redacted] E-Crimes labs. We evaluated the physical security and environmental controls including automated fire suppression systems, stand-alone fire extinguishers, monthly extinguisher inspections, Limited Area designations, electronic cipher locks, and cipher lock combination changes. We found nine physical security and environmental control weaknesses. Specifically, [redacted] (50 percent) [redacted] sites did not have signs designating them as Limited Areas, and the fire extinguishers at [redacted] (50 percent) [redacted] sites were not inspected on a monthly basis. In addition, E-Crimes labs at [redacted] (50 percent) [redacted] sites were not changing the cipher lock combinations in accordance with IRM policy. Finally, E-Crimes labs at [redacted] (75 percent) [redacted] sites were not secured by electronic cipher locks with audit capability. Figure 1 lists the control weaknesses found during our site visits.

Figure 1: Physical Security and Environmental Control Weaknesses at E-Crimes Labs

Physical Security and Environmental Controls	Number of Control Weaknesses
Automated Fire Suppression System	0
Stand-Alone Fire Extinguishers	0
[redacted]	[redacted]
Fire Extinguishers Inspection	2
[redacted]	[redacted]
[redacted]	[redacted]
Total	[redacted]

Source: Treasury Inspector General for Tax Administration's analysis of physical and environmental controls.

The IRM states that Limited Areas, which allow access to only authorized personnel with a verified business need, should have signs that prominently identify them.[11] The Occupational Safety and Health Administration requires portable fire extinguishers to be distributed for employee use every 75 feet or less and are to be inspected on a monthly basis.[12] The IRM also requires that CI evidence rooms have doors secured by electronic cipher locks with audit capability. [redacted] or when the combination potentially becomes compromised.

The Facilities Management and Security Services (FMSS) organization did not assess or review CI's assigned space, including the [redacted], in accordance with IRS policy.[13] The FMSS organization is responsible for planning, developing, implementing, evaluating, and controlling basic physical security concepts. FMSS section security chiefs are responsible for implementing and enforcing basic physical security concepts within their assigned territories. Further, the FMSS organization is required to complete a Facility Security Assessment Addendum that assesses IRS requirements at all locations where IRS employees are assigned.[14]

[redacted]

Recommendation 4: [redacted]

Management's Response: The IRS agreed with this recommendation. [redacted]

Recommendation 5: [redacted]

Management's Response: The IRS agreed with this recommendation. [redacted]

[11] IRM 10.2.14, *Methods of Providing Protection* (Aug. 29, 2019).

[12] U.S. Department of Labor, Occupational Safety and Health Administration*, Standard 1910.157, Portable Fire Extinguishers* (Nov. 2002).

[13] IRM 10.2.11, *Basic Physical Security Concepts* (Sept. 4, 2019).

[14] The Facilities Security Assessment Addendum is the IRS's process for evaluating and documenting credible threats, identifying vulnerabilities, and assessing the consequences for a specific facility.

[redacted]

*****************************2*************************
******2******

[redacted] To address the workspace requirements, E-Crimes section management proposed a consolidation of the number of E-Crimes labs using the existing regional area infrastructure and leaving two to three labs in each of the eight regions. The E-Crimes section does not have a definitive completion date because it is seeking to reduce the number of lab locations through employee attrition. An E-Crimes official stated that the consolidation would take at least five years to complete. We reviewed the December 2019 proposal for the nationwide reduction and consolidation of E-Crimes labs. The proposal states the desired lab locations for the consolidation and that the unconsolidated labs will be eliminated as opportunities arise. The proposal further states that current CISs would not be required to step down or relocate if not working from a desired consolidation location.

The E-Crimes section proposal states that the consolidation would reduce overhead costs such as utilities, equipment, and facility rental fees, but it did not quantify the costs or any potential savings from the consolidation effort. The FMSS organization[15] started looking at space options for the consolidation project in December 2019. The estimated project costs are $7 million and the estimated annual rent is $2.6 million. These estimates projected costs for incorporating locations into existing space acquisitions, but FMSS personnel stated those estimates might increase or decrease once the acquisition is finalized. Further, FMSS personnel had not identified any potential cost savings because it had not fully estimated the costs for all of the physical and environmental requirements for the new E-Crimes labs. Therefore, we were unable to determine whether potential cost savings would be achieved through the consolidation based on the information included in CI's proposal and additional information provided by FMSS personnel.

[15] The FMSS is responsible for the development and administration of long-term spacing strategy for the IRS.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether IRS CI is implementing effective security controls [redacted]

- [redacted]
- [redacted].
- Evaluated whether CI projected potential cost savings from reducing the number of E-Crimes labs through employee attrition by reviewing the E-Crimes consolidation proposal and high-level cost estimates.

Performance of This Review

This review was performed at the [redacted] during the period of February through July 2020. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Jason McKnight, Audit Manager; Khafil-Deen Shonekan, Lead Auditor; Andrea Nowell, Senior Auditor; and Daniel Preko, Auditor.

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 that the following internal controls were relevant to our audit objective: IRM policies related to physical, environmental, and logical controls over information technology and E-Crimes Standard Operating Procedures for digital evidence and environmental protection controls. We evaluated these controls by interviewing E-Crimes and FMSS personnel and reviewing relevant documentation, including policies and procedures related to the processing and storage of digital evidence, inventory records, and the E-Crimes consolidation proposal. We also conducted site visits to E-Crimes labs to evaluate physical and environmental controls and to examine [redacted] security controls.

Appendix II

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; [redacted] were not accounted for in the hardware asset inventory (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We met with CI personnel and identified [redacted] used to process digital evidence. We obtained two E-Crimes asset inventories and compared the forensic workstations we identified to the asset inventories. We found that four forensic workstations were not accounted for as required by the IRM.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; [redacted].

Methodology Used to Measure the Reported Benefit:

We met with E-Crimes personnel to determine the number and locations of the E-Crimes computer labs. We visited [redacted] computer labs used to analyze and store digital evidence and conducted physical walkthroughs of the labs to assess the physical security controls. We found that [redacted] labs visited did not [redacted] as required by the IRM.

Appendix III

Management's Response to the Draft Report

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

CRIMINAL INVESTIGATION

November 20, 2020

MEMORANDUM FOR: Deputy Assistant Inspector General for Audit

FROM: James C. Lee /s/ James C. Lee
Chief, Criminal Investigation

SUBJECT: Draft Audit Report for Audit 202020020, "Security Controls Over Electronic Crimes Labs Need Improvement"

Thank you for the opportunity to review and comment on the TIGTA Draft Report #202020020 – *"Security Controls Over Electronic Crimes Labs Need Improvement"*, dated September 28th, 2020. The IRS takes seriously our responsibility to ensure that all electronic crimes labs demonstrate proper controls with only the highest levels of security in mind. We are committed to adhering to all federal laws, regulations, and IRS policies, procedures, and guidelines that are applicable to the management of our electronic crimes labs.

We appreciate your review of our security controls and have attached a detailed response outlining the corrective actions that the IRS will take to address the recommendations. We have already taken action to address Recommendation #4. [redacted]

For the benefit of clarification, we would like to emphasize that CI has not jeopardized or put at risk any criminal investigation, even considering the corrective actions. [redacted] original evidence and criminal investigations are protected from risk of compromise.

Though correct in the recommendation that the CIO and CI need to develop protocols for forensic computers in CIS Labs, TIGTA's underlying basis is substantially flawed and draws misguided conclusions as to the potential impactsto the current forensic environment based on half-truth statements as CI outlined in our previous Comments

Matrix submission to TIGTA specifically with all unsupported statements made about potential vulnerabilities to CI's evidence collection and processing methodology in the report's pages 1 to 4. As noted in the paragraph above, the assurance of the hash value in ensuring a true copy of the original digital evidence as well as use of off-network forensic workstations mitigates the concerns raised. TIGTA' s basis for the development of CIS Lab protocols in the report should understand and allow for the CIS Labs' accepted law enforcement methods and means in conducting digital forensic analysis. Certain well-designed and accepted IT practices and standards outlined in the current IRM do not account for the necessary flexibility under which CIS Labs must be allowed to operate. IRS-CI attempted time and again to enlighten TIGTA to the uniqueness of CIS Labs' law enforcement mission which ended with the report's erroneous assumptions and conclusions impugning the CIS Labs in the audit report. The report's half-true statements and conclusions potentially undermine the CIS program, and the administration of justice especially as it relates to criminal tax law enforcement. We again ask for TIGTA's reconsideration and revision to the report's inflammatory statements and conclusions in the first four pages of the audit report.

Attached are our comments and responses to the recommendations. If you have any questions, please contact Executive Director of Technology Operations & Investigative Services, Patricia Ragano at 202-317-3687, or Deputy Director David Talcott at 703-986-2103.

Thank you.

Attachment

ATTACHMENT

RECOMMENDATION 1:
[redacted]

CORRECTIVE ACTIONS:
[redacted]

IMPLEMENTATION DATE:
July 15, 2022

RESPONSIBLE OFFICIAL(S):
Executive Director of CI's Office of Technology Operations & Investigative Services

CORRECTIVE ACTION(S) MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2:
The Chief, CI, should ensure that the hardware inventory requirements are clearly communicated and the inventory is updated as required.

CORRECTIVE ACTIONS:
The IRS Asset Management Project Office dictates the Service-wide policy for asset inventories. Their inventory plan requires an annual inventory, and GAO subsequently performs an annual audit. It is very likely that prior to required annual inventories, there will be discrepancies as noted by TIGTA in this report. In order to assure that the required annual inventories are updated as required, both the User Support and the Electronic Crimes Standard Operating Procedures (SOPs) will be updated and an inventory touchpoint between the two sections will occur on a quarterly basis. In effect, this will allow the required annual inventory to be completed more efficiently and ensure accuracy of EC/DF inventories.

These updated SOPs will be communicated to both the User Support and Electronic Crimes/Digital Forensics organizations.

IMPLEMENTATION DATE:
February 15, 2021

RESPONSIBLE OFFICIAL(S):
Executive Director of CI's Office of Technology Operations & Investigative Services

CORRECTIVE ACTION(S) MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3:
[redacted]

CORRECTIVE ACTIONS:
[redacted]

IMPLEMENTATION DATE:
Dependent upon funding.

RESPONSIBLE OFFICIAL(S):
Executive Director of CI's Office of Technology Operations & Investigative Services

CORRECTIVE ACTION(S) MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4:
[redacted]

CORRECTIVE ACTIONS:
[redacted]

IMPLEMENTATION DATE:
Implemented

RESPONSIBLE OFFICIAL(S):
Chief, Facilities Management and Security Services

CORRECTIVE ACTION(S) MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

5

RECOMMENDATION 5:
[redacted]

CORRECTIVE ACTION #5A:
[redacted]

IMPLEMENTATION DATE:
October 15, 2021

CORRECTIVE ACTION #5B:
[redacted]

IMPLEMENTATION DATE:
April 15, 2022

RESPONSIBLE OFFICIAL(S):
Chief, Facilities Management and Security Services

CORRECTIVE ACTION(S) MONITORING PLAN:
IRS will monitor this corrective action as part of our internal management system of controls.

Appendix IV

Office of Audit Comments on Management's Response

In response to our draft report, the Chief, CI, agreed with our recommendations, but stated that some of our underlying basis for making these recommendations is substantially flawed and draws misguided conclusions. We believe those statements warrant additional comment.

CI states that we are using half-truth statements, specifically "with all unsupported statements made about potential vulnerabilities to CI's evidence collection and processing methodology in the report's pages one through four." To this point, in the audit report we do not take a position on CI's evidence collection. Pages one through four of our report only discuss CI's evidence processing in a tangential manner. CI uses [redacted] to analyze digital evidence. Our audit work in this finding evaluated information technology security controls for those [redacted], not the collection, handling, or analyzing methodology of digital evidence. That being said, if [redacted] security controls are not in place there is an increased risk that data being analyzed could be compromised.

The facts presented in the first four pages of the report are documented and were independently reviewed. We conducted site visits and tested [redacted]. CI stakeholders did not dispute any of the conditions identified that led us to our conclusions and recommendations. [redacted] The IRM applies to all information and information systems in all offices and business, operating, and functional units within the IRS. While CI contends an inability to have certain information technology security controls in place due to law enforcement practices, we found instances in which the CISs effectively implemented the information technology security controls.

CI also states that our basis for the development of E-Crimes lab protocols should understand E-Crimes labs' law enforcement methods. We did not attempt to develop any protocols in our report. We understand that forensic workstations within E-Crimes labs may require flexibility to deviate from established IRS policies that govern most IRS information technology systems. For this reason, our recommendation provides the flexibility to identify and document accepted risks when exemptions to IRM policy are required. The Chief, CI, in conjunction with the Chief Information Officer, has agreed to do this.

We want to assure CI stakeholders that we did not report anything that should be interpreted as impugning or undermining the E-Crimes labs program. We appreciate the efforts and accommodations of all the stakeholders we met through the course of this audit. Most importantly, the corrective actions agreed upon by IRS stakeholders will enhance the E-Crimes lab program's risk management capabilities and their adherence to IRS information technology policies.

Appendix V

Glossary of Terms

Term	Definition
Access Controls	Policies uniformly enforced across all subjects, *i.e.,* users, and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: i) passing the information to unauthorized subjects or objects; ii) granting its privileges to other subjects; iii) changing one or more security attributes on subjects, objects, the information system, or system components; iv) choosing the security attributes to be associated with newly created or modified objects; or v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges, *i.e.*, they are trusted subjects, such that they are not limited by some or all of the above constraints.
Antivirus Signatures	A set of characteristics of known malware instances that can be used to identify known malware and some new variants of known malware.
Authentication	Verifies the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Cipher Lock	A lock, opened with a programmable keypad, used to limit and control access to a highly sensitive area.
Hot Fix	A single, cumulative package, which includes one or more files, that is used to address a problem in a product.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Network	An information system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Operating System	Software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function.
Patches	An update to an operating system, application, or other software issued specifically to correct particular problems with the software; software vendors issue patches to fix flaws that become apparent after their software has been released to the public.

Service Pack	A software program that corrects known bugs or problems or that adds new features. Typically released when the number of individual patches to the application becomes too large, Service Packs are easier to install than groups of patches.
Trojan Horse	A malicious program that pretends to be harmless in order to trick people into downloading it.
Virus	A piece of programming code usually disguised as something else that causes some unexpected and, for the victim, usually undesirable event and is often designed so it is automatically spread to other computers.
Worm	A type of malicious software program whose primary function is to infect other computers while remaining active on infected systems.

Appendix VI

Abbreviations

CI	Criminal Investigation
CIS	Computer Investigative Specialist
E-Crimes	Electronic Crimes
FMSS	Facilities Management and Security Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service