TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

While Renowned for Its Forensic Capabilities, the Digital Evidence Program Faces Challenges and Needs More Controls

April 30, 2008

Reference Number: 2008-10-106

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.

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

April 30, 2008

MEMORANDUM FOR CHIEF, CRIMINAL INVESTIGATION

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While Renowned for Its Forensics Capabilities, the Digital Evidence Program Faces Challenges and Needs More Controls (Audit # 200610029)

This report presents the results of our review of the Field Services computer forensics portion of the Criminal Investigation (CI) Division Electronic Crimes Program (E-Crimes).[1] The overall objective of this review was to determine whether E-Crimes properly controlled the collection and timely analysis of digital evidence in support of Internal Revenue Service (IRS) special agents. This audit was included in our Fiscal Year 2007 Annual Audit Plan and related to the Major Management Challenges of tax compliance initiatives and taxpayer protection and rights.

Impact on the Taxpayer

While E-Crimes enjoys an excellent reputation throughout the law enforcement community for digital evidence forensics, the absence of some Program-level processing controls has created risks that could compromise investigations in worst-case scenarios. As the volume of digital evidence significantly increases, the IRS must ensure that it treats this evidence properly and consistently to secure its admissibility in court.

Synopsis

E-Crimes' prominence in the investigative process has grown quickly, primarily because evidence of financial crimes is increasingly stored on computers, on portable electronic media, and at Internet storage facilities. Approximately 100 Computer Investigative Specialist (CIS)

[1] Appendix IV presents a Glossary of Terms used in the report.

agents stationed across all field offices provide technical expertise on digital evidence during the course of IRS criminal investigations.

We believe that the CIS agents' reputation for expertise and self-reliance has led E-Crimes to forgo establishing some common and necessary internal controls. For example, digital evidence is not backed up offsite, CIS agents are not required to keep a detailed record of their activities relating to an investigation, and digital or physical evidence in the possession of CIS agents is not periodically validated.

While our audit objective did not include a detailed assessment of the forward-looking strategies to maintain and advance the E-Crimes digital evidence program, we identified issues that could become problematic without management's attention, as demand for E-Crimes' services increases. The continued conversion of experienced special agents to CIS agents could intensify staff attrition concerns, requiring the CI Division to balance the need to have sufficient human capital resources to work criminal investigative priorities with the growing need for CIS agents. In addition, the Division's initiative to develop a new information technology infrastructure is considered essential to advancing digital evidence processing capabilities. Although information technology oversight is in place, the CI Division needs to ensure that non-technological risks are identified and systemically mitigated and that contingency plans are prepared, in case the new system does not provide the expected operational benefits or is delayed. Finally, the change to the supervisory structure for CIS agents will expand the administrative responsibilities of Area Lead Investigators, which must be considered when determining an effective span of control.

Grand jury secrecy rules precluded our review of whether E-Crimes analyzed digital evidence in a timely manner or followed appropriate legal provisions when seizing and processing digital evidence. The CI Division could not provide us with documentation or information relating to any grand jury investigation, which was the prevalent type of investigation in our audit's scope. Without such access, we could not satisfy our responsibility under generally accepted government auditing standards to obtain sufficient, appropriate audit evidence to provide a reasonable basis for findings and conclusions in these two areas.

Recommendations

We recommended that the Director, Electronic Crimes, protect digital evidence by 1) implementing a near-term disaster avoidance plan for digital data, 2) developing effective quality control guidelines and documentation standards for the forensic process, and 3) clarifying the role of the management information system as an evidence inventory control subject to periodic validation. In addition, we recommended that the Chief, Criminal Investigation, assess challenges to maintaining and advancing the digital evidence program by 1) testing the option of using non-law enforcement positions to benefit the field office role, 2) assigning responsibility to a task force or project management team regarding development of and contingency management for non-technological aspects of technology modernization, and 3) continuing to assess the span of control for first-line supervisors as the recently approved direct-line authority is implemented and experienced.

Response

IRS management agreed with Recommendations 2 through 6 and partially agreed with Recommendation 1. E-Crimes plans to 1) establish policy directives to require periodic validation of evidence data through supervisory operational reviews, 2) review its standard operating procedures annually, and 3) conduct operational reviews to develop quality control and documentation standards to include in future policy directives. In addition, the CI Division will monitor, re-evaluate, and adjust the span of control for the newly created direct-line supervisory positions as needed after standup of the organization. The CI Division will also ensure that project management teams for the information technology infrastructure project remain in compliance with the risk management process.

However, the CI Division believes that the information technology infrastructure project is near-term enough to facilitate the disaster avoidance plan we recommended, dependent on appropriate funding being available. Therefore, the CI Division does not agree that a distinct, near-term plan should be implemented prior to the completion of the information technology infrastructure project. The CI Division will continue to identify roles that can be accommodated with non-law enforcement personnel at E-Crimes' centralized support sites. However, the Division continues to believe that its current model of having experienced agents as CIS agents is most prudent and does not agree that non-law enforcement personnel can be considered for field offices. Management's complete response to the draft report is included as Appendix VI.

Office of Audit Comment

In two instances, we do not believe that the CI Division's corrective actions address the concerns in our recommendations. The Division plans to begin building data centers for the long-term data backup solution when funding is available. However, that will be only the start of implementation, not the completion. Funding for the data centers is scheduled for Fiscal Years 2009 and 2010, but funding for technology initiatives is dependent on the budget and might be at risk of not being fully approved. Without interim procedures, risks that could materialize from incidents or disasters will continue to exist over the next 2 years, or longer if the system is delayed. In addition, if the option of blending non-law enforcement personnel with experienced agents in the field is not piloted, CI Division management will be missing a valuable opportunity to maximize resources and minimize the risk of continued conversion of experienced special agents to CIS agents, thus exacerbating staff attrition concerns.

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

Nancy A. Nakamura, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Table of Contents

Appendices

Abbreviations

CI	Criminal Investigation
CIS	Computer Investigative Specialist
E-Crimes	Electronic Crimes Program
ECMIS	Electronic Crimes Management Information System
IRS	Internal Revenue Service

Background

The Electronic Crimes Program (E-Crimes) provides guidance and resources in securing, documenting, processing, maintaining, and presenting digital evidence[1] in support of Internal Revenue Service (IRS) criminal investigations. E-Crimes was established as a formal organizational component in 2001.[2] Since then, its role in the Criminal Investigation (CI) Division's law enforcement investigative process has expanded beyond digital data forensics at the field office level to include broad involvement in developing innovative uses of information technology. At the same time, there has been a large increase in demand for the more traditional mission of supporting the field office special agents in the collection and analysis of digital evidence. The digital evidence forensics services were the scope of this review.

The E-Crimes Field Services Program guides the efforts of approximately 100 special agents designated as computer investigative specialists (CIS agents), who are stationed across all CI Division field offices to provide technical expertise during the course of investigations. The CIS agents are not the lead IRS case agents for criminal investigations. Conceptually, they can be described as co-agents on a case. The degree to which digital data exist as a potential source of evidence in a particular investigation dictates the extent to which one or more CIS agents are involved in an investigation.

The IRS enjoys an excellent reputation in the digital evidence forensics area. For example, in 2004 an industry journalist described the IRS as arguably having the most sophisticated and efficient computer forensics teams, which are emulated by other government agencies.

CIS agents often extract and secure digital evidence from computers and other data storage devices when conducting court-approved search warrants at a person's residence, business, or other property.[3] The CI Division policy for collecting electronic records is to "image" information from a computer or other data device onto Federal Government digital hard drives but not to confiscate the electronic devices unless necessary. CIS agents will take possession of physical components only if they encounter problems accessing the data onsite or if a device itself is needed as evidence. CIS agent expertise includes using specialized equipment and

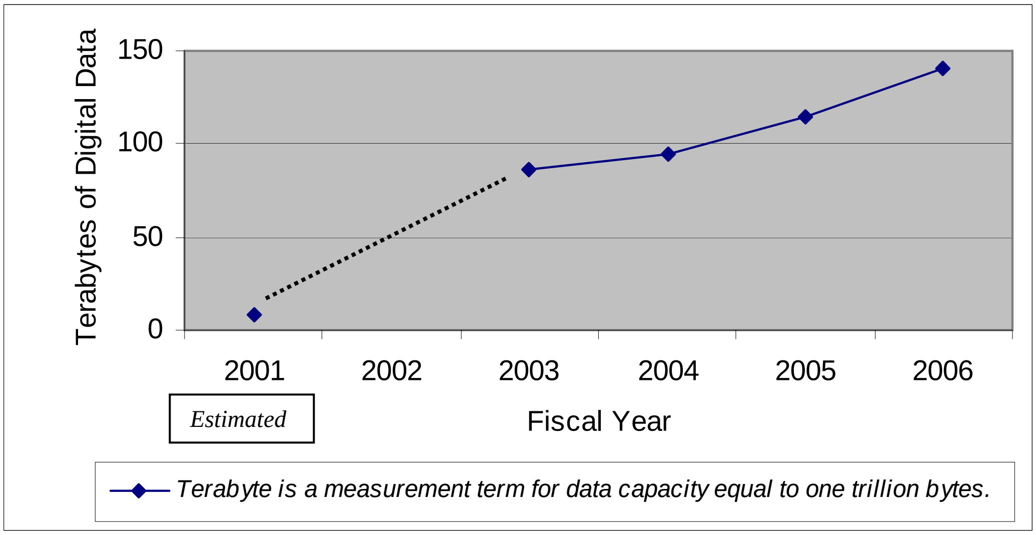
[1] Appendix IV presents a Glossary of Terms used in the report.
[2] E-Crimes was structured to integrate previously distinct Criminal Investigation Division programs under a common mission; establish program authority with a separate budget; and establish Headquarters-level guidance, policy, and direction.
[3] Not every investigation requires the execution of a search warrant. A person in possession of digital evidence can voluntarily consent to allow the IRS to search for and collect data. Other ways to obtain digital evidence without execution of a search warrant include a subpoena or summons, a witness or an informant, or an intercept from the Internet.

techniques to preserve digital evidence and to recover encrypted, password-protected, or hidden financial data. Normally, CIS agents will analyze the digital data collected and convert extracted evidence into a useable format for the investigating case agents. The information provided to case agents can include common word processing and spreadsheet files, database files, collections of image files, email system content, or even the creation of a virtual workstation that simulates the specific computer environment as it existed at the time of the data seizure.

Prior to establishment of E-Crimes, expertise and experience in computer technology had evolved in a decentralized manner, as agents provided technical support for field office operations. Tactical, day-to-day control of CIS agents remained with the respective local Special Agents in Charge. This supervisory arrangement continued after E-Crimes began operations. However, part of the restructuring involved the addition of geographically based Area Lead Investigators who report to the E-Crimes Headquarters Field Services Program, monitor CIS agents' workloads, and provide oversight and functional supervision to ensure proper coverage within their respective areas for all activities requiring the assistance of an electronic crimes investigator. A diagram of the posts-of-duty for E-Crimes personnel is presented in Appendix V. Because initial collection of digital data can require the efforts of several CIS agents working at the same site or simultaneously at multiple sites, large degrees of coordination and cooperation are necessary among individual CIS agents in the same vicinity and, at times, on a nationwide basis. This coordination is a significant part of an Area Lead Investigator's responsibilities in the Field Services Program.

E-Crimes' prominence in the investigative process has grown quickly, primarily because evidence of financial crimes is increasingly stored on computers, on portable electronic media, and at Internet storage facilities. E-Crimes estimated that the volume of digital data seized by CIS agents increased tenfold between Fiscal Years 2001 and 2003, and the upward trend has continued each year since (see Figure 1). This growth in volume represents hundreds of search warrants and the contents of thousands of data storage devices seized as evidence. E-Crimes management considers the increasing volume of digital evidence, which requires the use of specialized technical resources to support modern criminal investigations, as a major challenge to the Program.

Figure 1: Digital Data Seized Yearly by E-Crimes



Source: Totals calculated by the CI Division E-Crimes management information systems.

We performed this review at the Electronic Crimes Technology and Support Center laboratory in Springfield, Virginia, and at IRS office locations within the Baltimore, Maryland; Boston, Massachusetts; and Oakland, California, field offices during the period November 2006 through August 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. However, due to grand jury secrecy rules, we could not satisfy the Field Work Standard regarding sufficient, competent, and relevant evidence for some of our audit sub-objectives. The final section of the report presents an additional explanation of the scope limitation. 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. Except for the areas affected by grand jury limitations, we believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Electronic Crimes Program Has Not Established Sufficient Controls to Protect Digital Evidence

We believe that the CIS agents' reputation for expertise and self-reliance has led E-Crimes to forgo establishing some common and necessary internal controls. While CIS agents are renowned for their processing of digital evidence, the absence of specific Program-level controls has created risks that could compromise investigations in worst-case scenarios. The ultimate value of evidence in a criminal investigation is its admissibility in court. The process used by CIS agents to collect and secure digital data must protect the original image from inadvertent damage and allow the data analysis results to be authenticated as having come from the exact data that were initially obtained. Comprehensive internal controls are a means for ensuring that data are protected.

Since 2005, E-Crimes has used a task force to create and periodically revise standard operating procedures for the handling of digital evidence. E-Crimes personnel explained that the procedures were intentionally general enough to address the basic steps in collecting and processing digital evidence, without restricting the flexibility needed for each investigation's circumstances. Because of the experience and professional training that CIS agents have, E-Crimes management did not believe that they needed to, or could, dictate in detail how CIS agents should do their jobs. However, we believe that some procedures do not warrant being designated as discretionary actions and should not be omitted from the standard operating procedures.

The computer forensics principles that CIS agents are trained in are the basis for the processes they follow.

Digital evidence is not backed up offsite

CIS agents were not safeguarding a backup copy of the original evidence at a secure, offsite location. CIS agents made working copies of the digital data for analysis purposes, reserving the original images for any forensic authentication purpose that could become necessary to successfully prosecute the case. Both the original evidence images and the working copies were routinely stored within or near the CIS agents' workspaces. CIS agents retain custody of and safeguard the original digital evidence images from the time they are collected during a search warrant, or obtained through consent, until the completion of the investigation and any subsequent judicial actions.

Disaster avoidance and continuity principles require that effective data backup procedures include moving copies of critical data to an offsite location that would not be affected by a local catastrophic event such as fire, flood, natural disaster, sprinkler system malfunction, vandalism, or other intentional destructive acts. The location of the facility where the original evidence is stored can also increase the importance of offsite data backup. During our interviews, we observed that two of eight CIS agent workspace locations were below ground level. The IRS experienced the consequences of the risk inherent in below-ground facilities when its National Headquarters building was severely flooded in 2006. Data backup measures help to avoid situations that might otherwise cause loss of data, significant recovery expenses, decreased prosecution potential, or, ultimately, a loss of confidence in E-Crimes' reputation.

Digital images are normally written to and stored on digital hard drives similar to this example. Multiple images might fit on one hard drive, depending on their sizes.

E-Crimes management does value the concept of having an effective data storage and archival system for their Program. As described in a later section of the report, E-Crimes expects to implement within the next few years an information technology solution that would provide for dual location storage of digital evidence. However, in the current environment, E-Crimes management considers offsite backup for all digital images to be cost-prohibitive because the duplication of images would require additional physical space, equipment, data storage devices, and staff resources.

However, backup measures do not have to be costly or time-consuming. The most basic offsite backup process might require only data hard drives, which have become relatively inexpensive, and shipping postage for transport to another E-Crimes location. Digital hard drives can be recycled when data are subsequently determined to not warrant backup. In addition, E-Crimes could consider moving the current original evidence images to an offsite location to avoid the step of creating an additional copy. We believe that E-Crimes should identify interim procedures to help minimize or eliminate risks that could materialize from incidents or disasters.

CIS agents are not required to keep a detailed record of their activities relating to an investigation

While documentation principles are part of computer forensics training, the absence of specific baseline requirements in E-Crimes' standard operating procedures has left the methods and substance for documenting case activity during the course of an investigation to the discretion of individual CIS agents. The reporting requirement in the standard operating procedures simply states that CIS agents write memoranda and reports, as necessary, to document activities and to transmit the results of digital evidence analysis throughout the investigative and judicial processes. Our interviews revealed a variety of opinions held by CIS agents as to the necessity for case documentation. Most stated that they did not keep detailed written documentation to support their analyses or review results.

Several risks are inherent when careful records are not kept. Possible situations include 1) a CIS agent having to duplicate the analyses if it subsequently becomes necessary to provide detailed documentation or 2) difficulty in reassigning ongoing work to different CIS agents after analysis has begun. A practice of preparing reports only when necessary could prove detrimental to the investigation, with the passage of months or years between a CIS agent's analysis, recollections about such, and an eventual referral for prosecution.

E-Crimes must be prepared to help a prosecutor establish both the admissibility and persuasiveness of digital evidence. The Justice Department National Institute of Justice has issued a series of guides for law enforcement agencies that suggest general principles for handling digital evidence.[4] These guidelines are not mandated or official policy, but they represent the consensus of a computer forensics working group convened to consider common situations encountered during the examination of digital evidence. Repeated throughout these publications is the principal that documentation should be an ongoing process during the forensic examination. Digital forensics examiners should fully document all actions taken to process digital evidence and make examination notes available for review, discovery, or testimony purposes. The guidelines also suggest preparing a written report at the conclusion of an examination that outlines the process and pertinent data recovered. The rationale for these suggestions is that the examiner might need to testify about not only the conduct of the investigation but also the validity of the forensic procedures used.

The Justice Department concluded "a well-documented case is much more likely to result in a guilty plea, saving valuable prosecutorial and court resources."

E-Crimes management considered the responsibility for creating reasonably relevant processing notes to be inherent in computer forensic principles the CIS agents are trained in. E-Crimes management did not want to dictate a burdensome degree of documentation and report-writing requirements throughout an investigation because CIS agents collaborate with case agents as the theory of investigation evolves and provide additional digital evidence analysis as needed. Management expects CIS agents to provide for accurate recollection during the course of the investigation in the form of processing notes of steps taken, automated logs kept in forensic

[4] Publications of the United States Department of Justice, National Institute of Justice: *Electronic Crime Scene Investigation: A Guide for First Responders (July 2001)* (www.ojp.usdoj.gov/nij/pubs-sum/187736.htm), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement (April 2004)* (www.ojp.usdoj.gov/nij/pubs-sum/199408.htm), and *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors (January 2007)* (www.ojp.usdoj.gov/nij/pubs-sum/211314.htm).

processing applications, and written transmittals to case agents. Management believes that lack of adherence to this principle would be a performance issue for supervisors to address.

E-Crimes management stated that the issue involves how to define proper documentation and what form it should take throughout an investigation. We believe that E-Crimes' resistance to specifying those requirements has resulted in an environment in which documentation principles might not always be followed. For example, several E-Crimes personnel commented that the possibility of discovery during a trial was a reason for CIS agents to avoid maintaining detailed notes about their digital evidence processing. The concern was that if processing notes exist that the defense could review, there could be an opportunity for the defense to challenge the process in some manner. E-Crimes management agrees that to purposefully not make or retain notes for that reason is inappropriate and is not the policy of the E-Crimes Program.

We believe that E-Crimes should clearly set forth requirements in its standard operating procedures to ensure that properly documented case records support CIS agent activity at the time the analyses are conducted.

Digital or physical evidence in the possession of CIS agents is not periodically validated

CIS agents input information about digital images and other electronics-related evidence to the E-Crimes management information system (ECMIS). While the ECMIS, which was launched at the beginning of Fiscal Year 2006, was designed to provide evidence inventory accounting and case tracking information, the system has not yet evolved into a complete inventory control to account for digital data or to record disposition of the data. Inventory control principles require a periodic and independent validation of the physical condition of the items under control and reconciliation to inventory records to ensure the accuracy and reliability of the system. Exceptions identified through inventory controls can include missing and uncontrolled items.

Over the past several years, the CI Division has worked on some of the most notorious financial crime investigations in history, investigations that arguably contributed to fundamental changes to our economy and society. We believe that digital hard drives containing confidential and sensitive information, especially for cases of high national law enforcement priority, would be valuable items of contraband in the hands of an errant employee. In the worst case, only a single instance of compromised data in a high-profile investigation could damage the Federal Government's reputation and provide a way to mount a defense against criminal charges.

Chain-of-custody principles require CIS agents to maintain the integrity of evidence in its original condition and to ensure that the evidence is not lost, stolen, or altered in the months or years between the time obtained and any judicial proceedings. During a seizure action, the IRS prepares a search warrant inventory list that itemizes everything it has taken, including any digital images and electronics-related items. These lists are maintained in each investigation's case documentation. However, CI Division policy states that seized records and documentary evidence, including digital images, are not required to be tracked in the main IRS automated accounting system.[5] E-Crimes created the ECMIS to provide its own automated controls over digital evidence. E-Crimes personnel told us during our interviews that they entered evidence items in the ECMIS to capture workload attributes such as the location of the data when seized, the kinds of devices the data came from, and the digital size of the data.

To determine if the ECMIS was capable of tracking the electronic evidence inventory, we conducted a limited comparison of ECMIS evidence records to digital evidence on hand at the locations we visited. We were able to verify that 322 evidence items were present with the assigned CIS agents, as reflected in the ECMIS, and an additional 40 items had been disposed of or moved to a different location. If accountability for E-Crimes evidence was controlled, information on the 40 items would need to be updated. We believe that it is feasible for E-Crimes to use its existing evidence inventory database information for accountability purposes. This would represent an important control in monitoring the original digital evidence.

Recommendations

Recommendation 1: The Director, Electronic Crimes, should implement a near-term disaster avoidance plan for digital evidence in the possession of E-Crimes personnel, until a long-term plan is developed based on future technology advancements.

> ***Management's Response:*** The IRS agreed, in part, with the recommendation. In Fiscal Year 2009, E-Crimes plans to transition from the proof-of-concept testing stage to the implementation stage of its long-term information technology infrastructure project for the safe, efficient, and redundant storage of digital data. The CI Division believes that the information technology infrastructure project is near-term enough to facilitate the disaster avoidance plan in the recommendation. Implementation of this, or any, solution is dependent on appropriate funding.
>
> ***Office of Audit Comment:*** We do not believe that this corrective action addresses the concerns stated in our recommendation. The CI Division agreed that digital evidence is not backed up offsite but did not agree that a distinct, near-term disaster avoidance plan should be implemented prior to completion of the information technology infrastructure project. The Division plans to begin building data centers for the long-term solution when funding is scheduled to be available at the beginning of Fiscal Year 2009. However, that will be only the start of implementation, not the completion. Funding for the data centers is scheduled for Fiscal Years 2009 and 2010, but funding for technology initiatives is dependent on the budget and might be at risk of not being fully approved.

[5] For financial accounting reasons, seized currency, firearms, and property items that meet a specific minimum dollar value are required to be subject to systemic tracking. Digital evidence and traditional paper evidence are not considered to have any dollar value.

Without interim procedures, risks that could materialize from incidents or disasters will continue to exist over the next 2 years, or longer if the system is delayed.

Recommendation 2: The Director, Electronic Crimes, should include effective quality control guidelines and documentation standards in the E-Crimes standard operating procedures applicable to personnel nationwide.

Management's Response: The IRS agreed with the recommendation. In March 2008, E-Crimes issued revised standard operating procedures that address documentation standards applicable to the seizure and processing of digital evidence. E-Crimes plans to review the standard operating procedures annually. In addition, with the transition to direct-line management, E-Crimes plans to conduct operational reviews to develop quality control and documentation standards to include in future policy directives.

Recommendation 3: The Director, Electronic Crimes, should clarify the role of the ECMIS as an evidence inventory control and require a periodic evidence reconciliation and validation in the E-Crimes standard operating procedures.

Management's Response: The IRS agreed with the recommendation. With the recent transition to direct-line management of CIS agents within the Field Services Program, E-Crimes plans that one of the areas of focus for supervisors will be periodic validation of evidence data through operational reviews. E-Crimes plans to cover the requirements for such reviews and other administrative matters through forthcoming policy directives.

The Electronic Crimes Program Faces Challenges in Maintaining and Advancing Its Digital Evidence Program

Our audit objective did not include a detailed assessment of the CI Division's forward-looking strategies to maintain and advance the E-Crimes digital evidence program as the demand for E-Crimes' services increases. However, we identified three challenges that warrant management attention before they become problematic:

- The continued conversion of experienced special agents to CIS agents could intensify staff attrition concerns.
- The initiative to develop a new information technology infrastructure is considered essential to advancing digital evidence processing capabilities.
- The change to the supervisory structure for CIS agents will expand the administrative responsibilities of Area Lead Investigators.

The continued conversion of experienced special agents to CIS agents could intensify staff attrition concerns

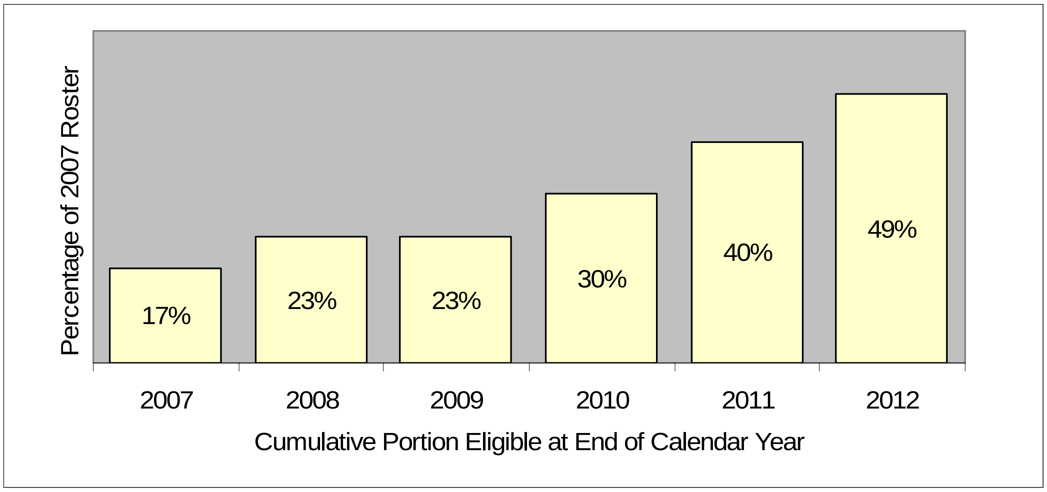
The CI Division selects from its pool of experienced special agents who have demonstrated information technology skills when filling CIS agent positions. Gaining an experienced agent in the CIS agent position benefits the E-Crimes program but might represent a detriment to the field office that loses the experienced special agent from its ranks. The CI Division prefers this method of in-house staffing as opposed to having technically educated, but non-law enforcement, personnel perform digital evidence analyses. E-Crimes believes that the CIS agent's job is not only to preserve, extract, and analyze the digital evidence but also to know what to look for, what questions to ask, and how to prepare evidence for a trial. In addition, because they are law enforcement agents, CIS agents can carry firearms, execute warrants, and perform searches and seizures.

We agree with E-Crimes' contention that the law enforcement background makes experienced special agents likely to be the best possible CIS agents. However, we believe that the accelerated growth in the volume of digital evidence in the investigative process warrants reconsideration of the alternative of also hiring technologically educated, but non-law enforcement, personnel to blend with experienced agents and fill some aspects of the field office CIS agent role. Because of uncertainty as to how high the volume of digital data seized will rise, how long special agent attrition will exceed hiring authority, and how successful technological solutions will be in maximizing the use of CIS agent resources, we believe that the CI Division will have to balance the need to have sufficient human capital resources to work criminal investigative priorities with the growing need for CIS agents.

Selection as a CIS agent dedicates a special agent to a collaborative support role and removes him or her from the primary case agent role.

Figure 2 shows our estimate that nearly one-half of the CIS agents and Area Lead Investigators on rolls at the beginning of Calendar Year 2007 will be eligible to retire by the end of 2012, based on retirement eligibility dates. Under the current selection process, agents selected to replace retiring CIS agents will be taken from the pool of experienced field office investigative agents.

Figure 2: Forecast of Retirement Eligibility



Source: Our comparison of the E-Crimes Personnel Roster (January 2007) to retirement eligibility dates in the Department of the Treasury automated personnel system.

Since 2002, overall attrition has exceeded or matched overall hiring in the CI Division due to budgetary limitations. At the time of our audit, the CI Division anticipated losing about 150 special agents in each of the next 2 years, and it expected to hire only 46 and 48 new agents in Fiscal Years 2007 and 2008, respectively. The attrition of human capital is a significant management challenge affecting many parts of the IRS, not just the CI Division. In the past 2 years, we have expressed our concern that the loss of experienced special agents might adversely affect the overall levels of and improvements in productivity that the CI Division had been experiencing.[6] In this environment, we believe that E-Crimes should determine whether a deviation from its policy of in-house CIS agent recruiting is warranted, especially over the longer term. In addition, E-Crimes should contact other digital forensics functions to identify best practices in staffing and recruiting.

The initiative to develop a new information technology infrastructure is considered essential to advancing digital evidence processing capabilities

The CI Division has started an initiative to develop a technological solution because it continues to encounter increasing volumes of digital evidence. To monitor the planning, development, and implementation milestones of new technology solutions, the CI Division has established an Information Technology Executive Steering Committee and Governance Process. This Process provides oversight to the technological aspects of the planned infrastructure, but it is not designed to focus on how the infrastructure will affect non-technological aspects. The

[6] *Statistical Portrayal of the Criminal Investigation Function's Enforcement Activities From Fiscal Year 2000 Through Fiscal Year 2006* (Reference Number 2007-10-083, dated June 6, 2007).

Government Accountability Office has issued guidance for agencies to include comprehensive risk management as a key element when undertaking new projects, including the initiative's impact on non-technological elements (people, processes, physical infrastructure).[7]

The CI Division has obtained funding for its initiative in the IRS Information Technology Modernization Vision and Strategy for Fiscal Years 2009 and 2010. If prototype testing is successful, the proposed system will include the buildout of 2 full-scale digital evidence data centers, estimated at the time of our audit to exceed $3 million each. The data centers will store and archive digital evidence, perform analysis, and deliver results electronically to case investigators in field offices nationwide. The system will leverage state-of-the-art information technology to use available E-Crimes resources to meet the increasing need to exploit digital evidence in complex financial investigations. The data centers will change the handling of digital data but not eliminate the need for the cadre of CIS agents in the field office locations to capture the data at their sources.

The IRS should have contingency plans, in case the new system does not provide the expected operational benefits.

As acknowledged in the Modernization Strategy, the IRS has had some difficulty with its overall information technology modernization. Indeed, history shows that Federal Government technology initiatives are prone to various risks that influence the predictability of the eventual timeliness or functionality of a project. For other CI Division technology initiatives, task forces have been created to assist in the projects' formulation.[8] Task force members represented various levels of the organization: managers, special agents, support positions, and information technology specialists. At the time of our review, such a task force had not been formed for the data center initiative. We believe that in addition to the formal IRS information technology oversight in place, the CI Division needs a task force to ensure that 1) non-technological risks are identified and systematically mitigated, 2) personnel are prepared for process changes that will accompany the new system, and 3) contingency plans are prepared, in case the new system does not provide the expected operational benefits or is delayed. This initiative is a significant challenge because E-Crimes officials believe that the advancement of digital evidence processing capabilities is essential to maintaining the CI Division's ability to conduct effective investigations as technology advances.

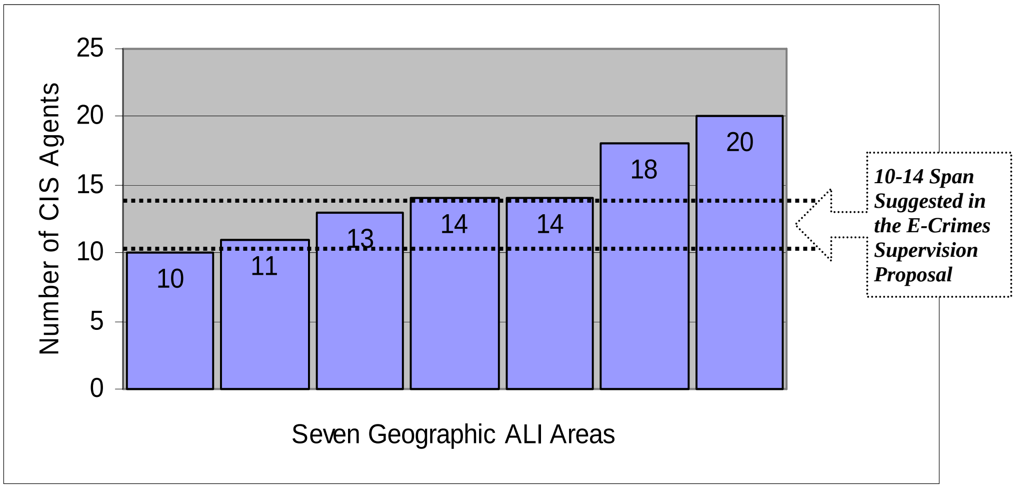
[7] "Key IT System Acquisition Best Practices" identified and reported by the Government Accountability Office: *Information Technology: DOD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls, Appendix II* (GAO-04-722, dated July 2004) or *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System, but Improvements Still Needed, Appendix II* (GAO-07-912, dated July 2007).

[8] The Investigative Data Analytics Project and the Scanning and Document Management Project, as noted in the Criminal Investigation Business Performance Report (dated March 31, 2007).

The change to the supervisory structure for CIS agents will expand the administrative responsibilities of Area Lead Investigators

At the time of our audit, E-Crimes was proposing the formal transfer of supervisory responsibility for the approximately 100 CIS agents from field office managers to a direct line of authority within E-Crimes. This change in management structure was approved by the Chief, CI, on October 24, 2007, and will be implemented over the following several months. The rationale for this proposal was that E-Crimes would manage CIS agent resources better than field office managers who have had no formal training in computer forensics or the peculiarities of digital evidence. In addition, the E-Crimes reorganization proposal outlined the need to add one more Area Lead Investigator position to address the span of control disparity.[9] Figure 3 shows that two of the seven Area Lead Investigator positions had significantly more CIS agents to oversee than their counterparts.

Figure 3: Span of Control for Area Lead Investigators



Source: E-Crimes Personnel Roster (January 2007). ALI = Area Lead Investigator.

Our interviews with personnel in one of the two high span-of-control areas revealed that the higher number of agents and larger geographic coverage issues significantly limited detailed supervisory oversight of the CIS agents. Consequently, the Area Lead Investigator had to rely on the proficiency of the CIS agents to perform their duties without close supervisory involvement. E-Crimes personnel advised us that this situation could become even more challenging as the number of digital evidence seizures continues to rise at an exponential rate, potentially bringing with it the need for additional CIS agents in the future.

[9] The proposal also establishes a new name and personnel system codes to replace the non-supervisory Area Lead Investigator positions with expanded supervisory positions.

Because implementation of direct-line authority between CIS agents and Area Lead Investigators will create additional administrative responsibilities for Area Lead Investigators as the official first-line managers, we are concerned that achieving the proper degree of supervisory involvement will remain a challenge after the management restructuring. We believe that E-Crimes should conduct an online assessment as the new management structure is implemented to ensure that the spans of control, both geographically and staffing related, do not jeopardize the uniform management of the digital forensics program.

Recommendations

Recommendation 4: The Chief, CI, should ensure that E-Crimes tests the option of using non-law enforcement positions to benefit the digital evidence field office role.

> ***Management's Response:*** The IRS agreed with the recommendation. The CI Division believes that non-law enforcement personnel should be considered where feasible to support or augment the role of CIS agents in the field locations. However, the CI Division is unsure how the recommended option of using non-law enforcement positions to benefit the digital evidence field office role can be tested. It has considered this option but continues to believe that the current model of having experienced special agents as CIS agents is most prudent due to the technological, legal, investigative, and financial requirements of the CIS agent position. However, the CI Division will continue to identify roles that can be accommodated with non-law enforcement personnel at the E-Crimes support center as well as the data centers.
>
> ***Office of Audit Comment:*** We do not believe that this corrective action addresses the concerns stated in our recommendation. The CI Division agreed to continue considering non-law enforcement personnel for centralized support positions but did not agree that non-law enforcement personnel can be considered for positions in field offices to benefit the digital evidence role of CIS agents. If the option of blending non-law enforcement personnel with experienced agents in the field is not piloted, CI Division management will be missing a valuable opportunity to maximize resources and minimize the risk of continued conversion of experienced special agents to CIS agents, thus exacerbating staff attrition concerns.

Recommendation 5: The Chief, CI, should ensure that E-Crimes specifically assigns to a task force or project management team the responsibility of having a structured and documented risk management process for the information technology infrastructure project to address non-technological aspects and contingency plans.

> ***Management's Response:*** The IRS agreed with the recommendation. The CI Division already has in place an information technology project management team as well as an internal E-Crimes team composed of management officials, CIS agents, and technical experts. The CI Division believes that these teams comply with the risk

management process that was recommended and will ensure that the teams remain in compliance.

Recommendation 6: The Chief, CI, should ensure that E-Crimes continues to assess the scope of the responsibilities of the revised Area Lead Investigator positions as direct-line authority is implemented and experienced to determine an effective span of control that addresses long-term organizational needs.

Management's Response: The IRS agreed with the recommendation. The CI Division will monitor the issue, re-evaluate the span of control for the newly created direct-line management position after standup of the organization, and adjust the span of control if needed.

Grand Jury Secrecy Rules Precluded an Effective Review of Data Analysis Timeliness or Application of Seizure Provisions

Because of grand jury secrecy rules,[10] the CI Division could not provide us with documentation or information relating to grand jury investigations. Without such access, we could not satisfy our responsibility under generally accepted government auditing standards to obtain and evaluate sufficient audit evidence to support conclusions as to whether E-Crimes analyzed digital evidence in a timely manner or followed appropriate legal provisions when seizing and processing digital evidence. We do not provide any assurances or recommendations in these two areas.

This grand jury scope limitation is prevalent in our audits of the CI Division. Due to the nature of non-tax crimes within the CI Division's jurisdiction, most investigations are conducted jointly with at least one other Federal Government law enforcement agency and use the grand jury process to facilitate the investigations. The CI Division's position, based on advice from the IRS Office of Chief Counsel, Division Counsel/Associate Chief Counsel (Criminal Tax),[11] was that when the classification of material as grand jury or non-grand jury is in question, the ultimate decision to release information rests with the attorney for the Federal Government (such as the United States Attorney's Office or other pertinent Department of Justice official). We did not get permission to review supporting documents on grand jury investigations from the applicable United States Attorney Offices for the IRS field offices we visited.

As a result, the scope of cases subject to our review of supporting documentation consisted of only 11 non-grand jury investigations (9 were in a single field office, and 6 were assigned to a single CIS agent), as opposed to our planned audit sample scope of 30 investigations from

[10] Federal Rules of Criminal Procedure, 18 U.S.C. Appendix Rule 6 (2005) state that persons shall not disclose matters occurring before the grand jury.

[11] A function within the IRS Office of Chief Counsel responsible for providing legal guidance.

3 dispersed field offices. We did not observe anything noteworthy in the case actions when we reviewed the documentation for the 11 non-grand jury investigations.

The legal provisions applicable to the seizure of digital evidence in criminal investigations are based on the Fourth Amendment to the United States Constitution and other statutory privacy laws. CIS agents help to ensure that appropriate legal requirements are met by assisting the special agents in drafting search warrant applications with proper language to describe computer hardware, software, peripherals, and data stored within the computers to be seized. Subsequently, CIS agents must comply with any warrant and local judicial time requirements for timely review or return of seized media evidence within the scope of the warrant. Even in the absence of judicial requirements, E-Crimes strives for digital evidence analysis to be completed within a short period to minimize the elapsed calendar days for an investigation.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to determine whether the CI Division E-Crimes[1] properly controlled the collection and timely analysis of digital evidence in support of IRS special agents. To accomplish this objective, we planned to evaluate internal controls regarding the processing of digital data obtained by E-Crimes and to review documentation supporting the activity of the E-Crimes CIS agents during their assignments.

As discussed in the final section of the audit report, grand jury secrecy rules limited the scope of our review for two sub-objectives in our audit plan. The scope limitation meant that we could not conduct some planned tests in accordance with the generally accepted government auditing standard regarding the Field Work Standard for Performance Audits. This Standard relates to our need to have sufficient audit evidence with which to provide a reasonable basis for findings and conclusions. Because we could not have access to any documentation of CIS agent activity on grand jury investigations, we could not conclude whether E-Crimes analyzed digital evidence in a timely manner or followed appropriate legal provisions when seizing and processing digital data.

To accomplish the audit objective, we:

I. Evaluated internal controls relating to digital evidence obtained or seized by CIS agents.

   A. Reviewed the Internal Revenue Manual, the standard operating procedures, and other guidance relating to securing and analyzing digital evidence.

   B. Used a copy of the ECMIS[2] data as of January 12, 2007, to establish the population of digital evidence assignments in which CIS agents were involved during Fiscal Year 2006. We considered the reliability of data contained in the ECMIS to be undetermined in terms of completeness and accuracy. However, we determined that using the data for informational purposes would not weaken our analysis or lead to an incorrect or unintentional message.

[1] Appendix IV presents a Glossary of Terms used in the report.

[2] At the time of our audit, E-Crimes considered the ECMIS to still be in pilot status. E-Crimes had only recently completed a validation effort to gain confidence in the content of the ECMIS, after launching the System subsequent to the beginning of Fiscal Year 2006.

C. Observed the physical environments for digital evidence analysis and storage during onsite visits to three selected field offices.[3]

   1. Judgmentally selected the Baltimore, Maryland; Boston, Massachusetts; and Oakland, California, field offices as audit sites, based on ECMIS data that indicated high totals for the number of investigations assisted on, number of evidence items seized, and volume of digital data seized. We also considered whether some of the investigations were potentially non-grand jury investigations and ensured that the selected locations were geographically dispersed. At least three different CIS agents within each selected field office had been the primary CIS agent for several digital analysis investigations during Fiscal Year 2006.

   2. Judgmentally selected for visitation the posts-of-duty for three Area Lead Investigators and nine CIS agents, located in eight cities, within the three selected field offices. We did not physically visit other CIS agent posts-of-duty within those field offices because they were in outlying geographical locations, were staffed by less experienced CIS agents, or could not be scheduled during the time of our visit.

D. Interviewed each selected Area Lead Investigator and CIS agent to gain their perspectives on various aspects of the digital data forensics environment.

E. For investigations in which 8 selected CIS agents were the primary CIS agents, verified whether 362 evidence items recorded in the ECMIS were accounted for properly. The verification process was limited because all investigation names relating to grand jury investigations had to be covered from our view. Because we could not handle the evidence items ourselves, we had to rely on the CIS agents to translate names into case numbers and to orally read evidence label information for our use.

II. Reviewed documentation regarding CIS agent activity on Fiscal Year 2006 assignments.

A. Reviewed monthly time reports for the period October 2005 through February 2007 for each CIS agent in the selected field offices to determine the number of hours charged to specific investigations, projects, or other time categories.

B. Reviewed relevant case documentation on non-grand jury investigations assigned to the CIS agents visited. Only 11 (12 percent) of the 94 investigations assigned to the

[3] There were 30 field offices designated in the ECMIS at the time of our audit. However, the CI Division was in the process of consolidating some field offices.

8 CIS agents on the ECMIS were non-grand jury. Of these 11 investigations, 9 were in 1 field office and 6 were assigned to 1 CIS agent. We reviewed paper documentation from the CIS agents' case files for the 11 non-grand jury investigations to evaluate CIS actions and the timeline of the assignment.

C. Via letters, requested the assistance of three applicable United States Attorney's Offices in determining, for grand jury investigations, whether CI Division documents that could be responsive to our audit tests were actually grand jury material.

Appendix II

Major Contributors to This Report

Nancy A. Nakamura, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)
Carl L. Aley, Director
John R. Wright, Director
Diana M. Tengesdal, Audit Manager
Timothy A. Chriest, Lead Auditor
Joseph P. Smith, Senior Auditor
Ahmed M. Tobaa, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Director, Technology Operations and Investigative Services, Criminal Investigation SE:CI:TOIS
Deputy Director, Technology Operations and Investigative Services, Criminal Investigation SE:CI:TOIS
Director, Electronic Crimes, Criminal Investigation SE:CI:TOIS:EC
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Planning and Strategy, Criminal Investigation SE:CI:S:PS

Appendix IV

Glossary of Terms

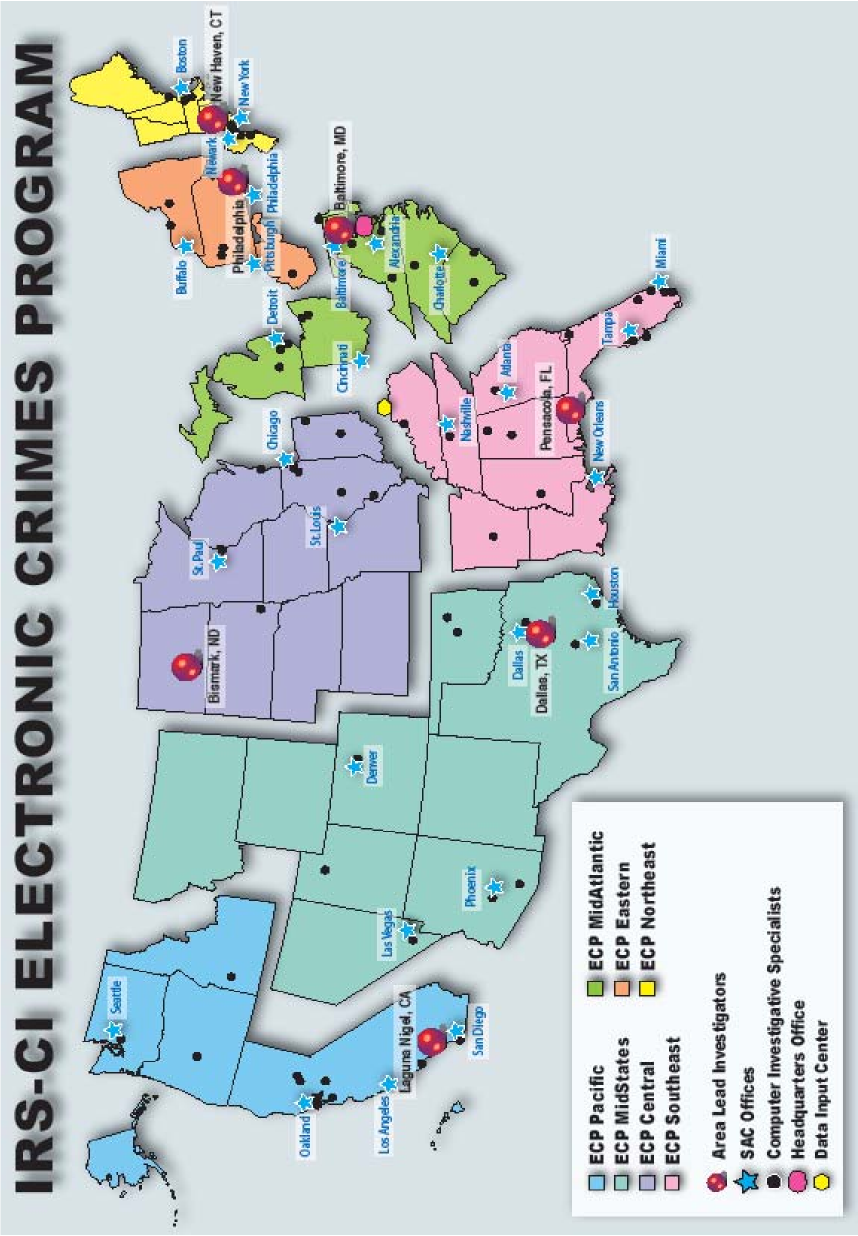
Term	Definition
Area Lead Investigator	Reports directly to the E-Crimes Director, Field Services. In direct coordination with the field offices, the Area Lead Investigator provides national program direction, resource allocation, knowledgeable oversight, and functional supervision of CIS agents to ensure timely and quality workload management, completion of assignments, training, and support.
Computer Investigative Specialist (CIS)	An experienced special agent with excellent financial investigative skills and knowledge of accounting and legal principles. A CIS agent completes a standardized course of study in computer evidence recovery and analysis. The mission of the CIS agent position is to serve as an investigator who contributes computer expertise to criminal investigations. A CIS agent is a member of his or her respective field office and should be used exclusively for CIS agent assignments.
Criminal Investigation (CI) Division	Responsible for investigating alleged violations of criminal statutes regarding tax administration, which is relatively evident because of the widely known role of the IRS as the nation's tax collection agency. In addition to working tax evasion cases, IRS agents often work with financial components of other Government agencies to combat money laundering, corporate fraud, terrorism financing, currency reporting violations, narcotics, or other critical national law enforcement priorities.
Digital Data	Information contained on a digital storage device.
Digital Evidence	Information of investigative value, stored or transmitted in digital form, that may be relied upon in court.

Term	Definition
Discovery	A legal term for the pretrial process during which each party requests relevant information and documents from the other side, in an attempt to "discover" pertinent facts. Discovery methods include depositions, requests for admissions, document production requests, and requests for inspection.
Electronic Crimes Management Information System (ECMIS)	An electronic case management system designed by E-Crimes specifically to capture workload data related to the acquisition of digital evidence from whatever source and the processing of that evidence by a CIS agent in support of an investigation.
Electronic Crimes Technology and Support Center Laboratory	The post-of-duty for some E-Crimes Headquarters management officials and the defacto home location for E-Crimes. Laboratory personnel evaluate, test, and document the effectiveness and validity of computer forensics procedures, techniques, equipment, and software used in the data recovery and analysis processes. The laboratory also develops basic and advanced training programs for CIS agents.
Field Office	Offices within the five CI Division geographical areas throughout the country with boundaries that range from a portion of a single State to inter-State areas. There were 30 CI Division field offices at the time of our audit. Each field office has a Special Agent in Charge to direct, monitor, and coordinate the criminal investigation activities within that office's area of responsibility. Several post-of-duty cities are located within each field office.
Field Services Program	Under the Director, Field Services, supervises the Area Lead Investigators and is responsible for the coordination and direction of E-Crimes Field Operations nationwide.
Forensics	Involves obtaining and analyzing information for use as evidence in court. Computer forensics involves scientifically analyzing data from digital storage media, including the recovery of data that users have hidden or deleted. Investigators often examine digital data not knowing if the data contain evidence or if any evidence would be incriminating or would disprove an allegation.

Term	Definition
Hard Drive	A sealed box containing rigid platters (disks) coated with a substance capable of storing data magnetically in digital format. One or more hard drives can be present inside the case of a computer and can exist in standalone, external cases attached by cables. A hard drive normally stores information such as computer programs, text, pictures, video, and multimedia files.
Image	In a data forensics context, a duplicate copy of an entire digital data storage device exactly as it existed in digital form. When a computer file is saved, it actually exists in randomly scattered sectors on the disk rather than in one continuous block. When a file is retrieved, the scattered pieces are reassembled from the disk in the device's memory and presented as a single file. Imaging copies all the scattered pieces of various files, even fragments of deleted files. In contrast, a file-by-file copy merely creates a copy of reassembled files without including file fragments.
Log Data	As a generic term, refers to a computer application's automated recording of user; computer networking; or computer operating activity that might contain software installation and setting information, user registration data, or a running account of a computer process.
Modernization Vision and Strategy	A tool to support the fulfillment of the IRS mission and strategic goals by establishing a 5-year plan that drives information technology investment decisions. The Modernization Strategy issued in October 2006 will guide the investment priorities of the Business Systems Modernization program for Fiscal Years 2007 through 2011.
Special Agent	A duly sworn CI Division Federal Government law enforcement officer trained as a financial investigator.

Appendix V

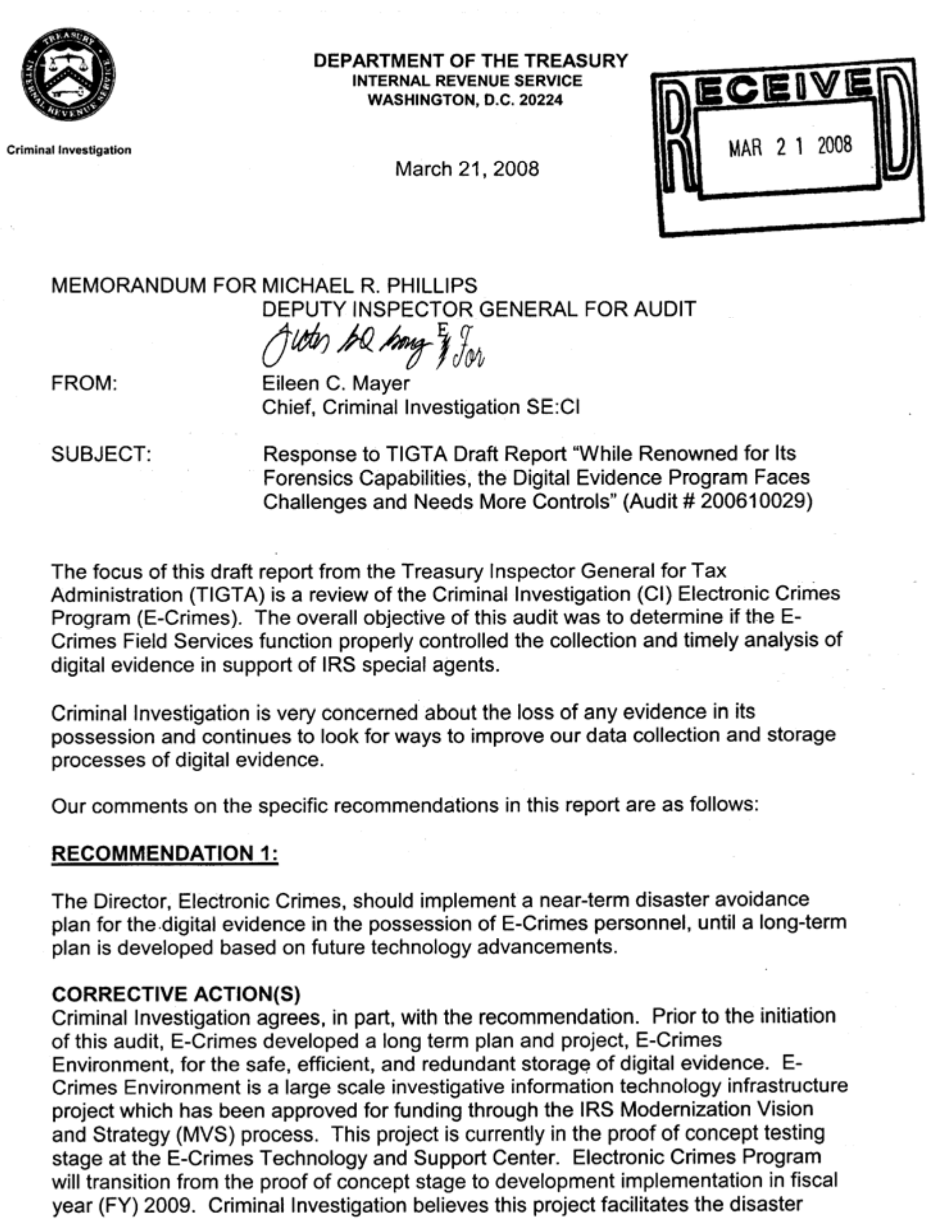
Electronic Crimes Program Post-of-Duty Map



Source: Diagram by E-Crimes (January 2007). ECP = Electronic Crimes Program. SAC = Special Agent in Charge.

Appendix VI

Management's Response to the Draft Report



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

Criminal Investigation

March 21, 2008

MEMORANDUM FOR MICHAEL R. PHILLIPS
DEPUTY INSPECTOR GENERAL FOR AUDIT

For

FROM: Eileen C. Mayer
Chief, Criminal Investigation SE:CI

SUBJECT: Response to TIGTA Draft Report "While Renowned for Its Forensics Capabilities, the Digital Evidence Program Faces Challenges and Needs More Controls" (Audit # 200610029)

The focus of this draft report from the Treasury Inspector General for Tax Administration (TIGTA) is a review of the Criminal Investigation (CI) Electronic Crimes Program (E-Crimes). The overall objective of this audit was to determine if the E-Crimes Field Services function properly controlled the collection and timely analysis of digital evidence in support of IRS special agents.

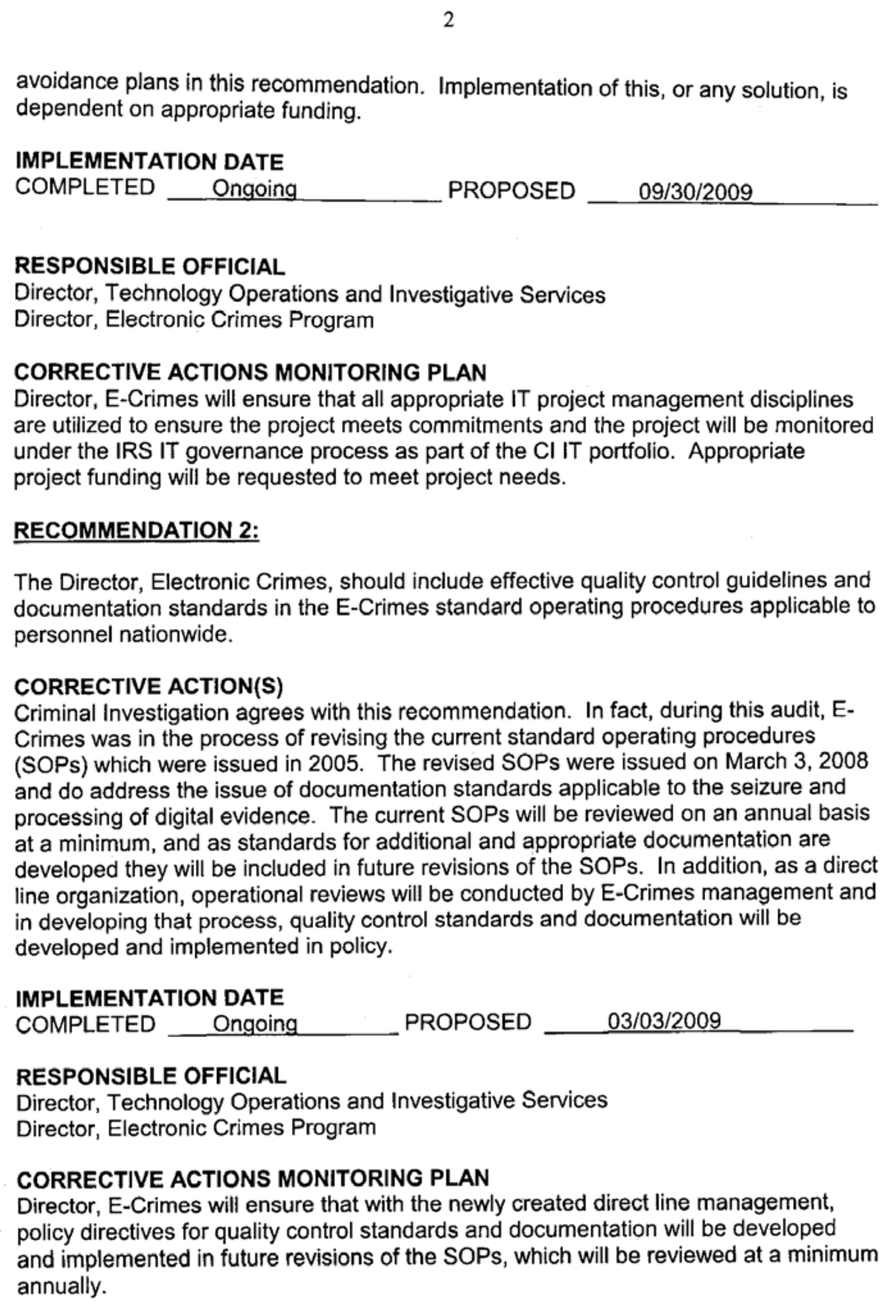
Criminal Investigation is very concerned about the loss of any evidence in its possession and continues to look for ways to improve our data collection and storage processes of digital evidence.

Our comments on the specific recommendations in this report are as follows:

RECOMMENDATION 1:

The Director, Electronic Crimes, should implement a near-term disaster avoidance plan for the digital evidence in the possession of E-Crimes personnel, until a long-term plan is developed based on future technology advancements.

CORRECTIVE ACTION(S)
Criminal Investigation agrees, in part, with the recommendation. Prior to the initiation of this audit, E-Crimes developed a long term plan and project, E-Crimes Environment, for the safe, efficient, and redundant storage of digital evidence. E-Crimes Environment is a large scale investigative information technology infrastructure project which has been approved for funding through the IRS Modernization Vision and Strategy (MVS) process. This project is currently in the proof of concept testing stage at the E-Crimes Technology and Support Center. Electronic Crimes Program will transition from the proof of concept stage to development implementation in fiscal year (FY) 2009. Criminal Investigation believes this project facilitates the disaster



2

avoidance plans in this recommendation. Implementation of this, or any solution, is dependent on appropriate funding.

IMPLEMENTATION DATE
COMPLETED ___Ongoing___________ PROPOSED ____09/30/2009___________

RESPONSIBLE OFFICIAL
Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN
Director, E-Crimes will ensure that all appropriate IT project management disciplines are utilized to ensure the project meets commitments and the project will be monitored under the IRS IT governance process as part of the CI IT portfolio. Appropriate project funding will be requested to meet project needs.

RECOMMENDATION 2:

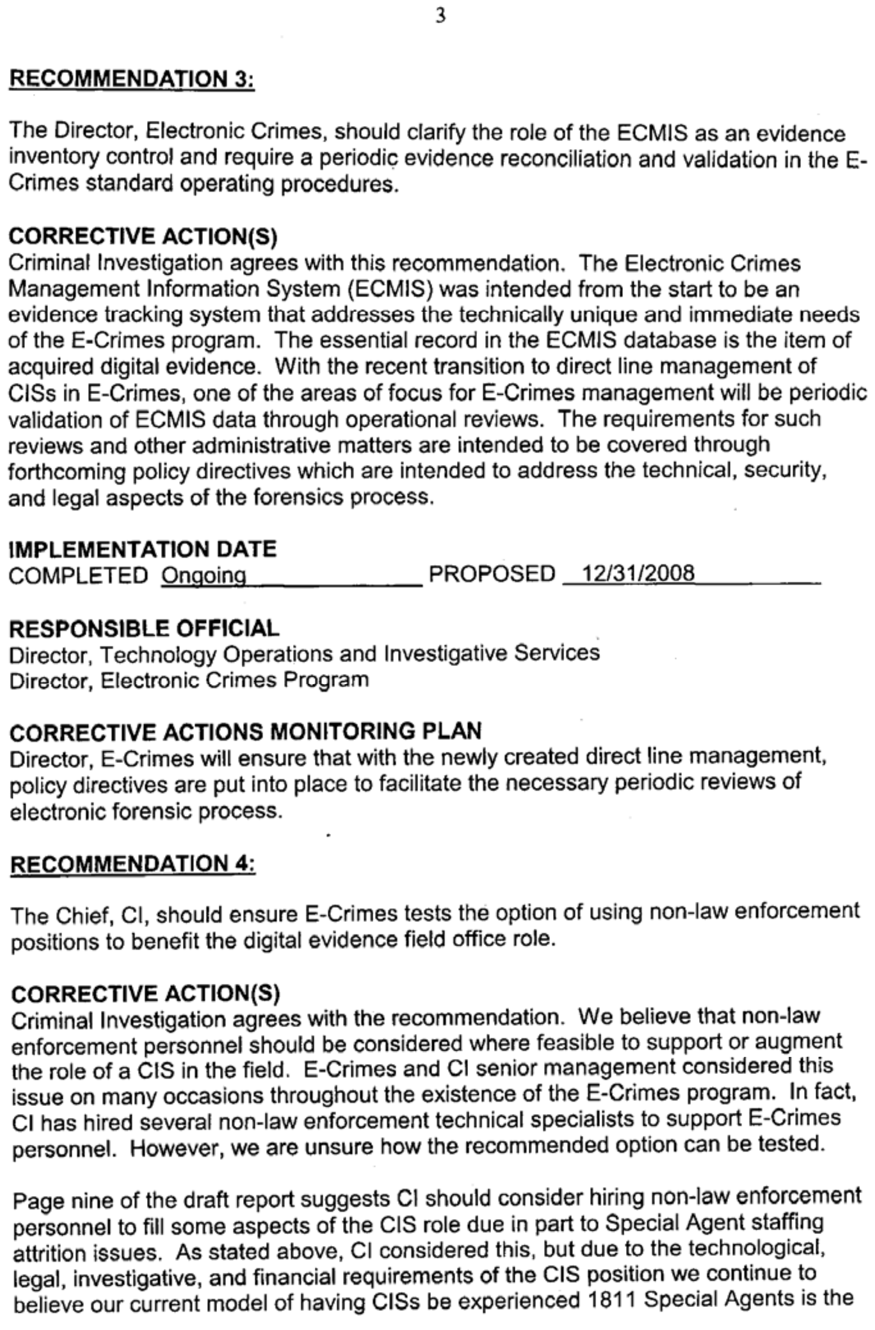
The Director, Electronic Crimes, should include effective quality control guidelines and documentation standards in the E-Crimes standard operating procedures applicable to personnel nationwide.

CORRECTIVE ACTION(S)
Criminal Investigation agrees with this recommendation. In fact, during this audit, E-Crimes was in the process of revising the current standard operating procedures (SOPs) which were issued in 2005. The revised SOPs were issued on March 3, 2008 and do address the issue of documentation standards applicable to the seizure and processing of digital evidence. The current SOPs will be reviewed on an annual basis at a minimum, and as standards for additional and appropriate documentation are developed they will be included in future revisions of the SOPs. In addition, as a direct line organization, operational reviews will be conducted by E-Crimes management and in developing that process, quality control standards and documentation will be developed and implemented in policy.

IMPLEMENTATION DATE
COMPLETED ___Ongoing_________ PROPOSED _____03/03/2009__________

RESPONSIBLE OFFICIAL
Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN
Director, E-Crimes will ensure that with the newly created direct line management, policy directives for quality control standards and documentation will be developed and implemented in future revisions of the SOPs, which will be reviewed at a minimum annually.



3

RECOMMENDATION 3:

The Director, Electronic Crimes, should clarify the role of the ECMIS as an evidence inventory control and require a periodic evidence reconciliation and validation in the E-Crimes standard operating procedures.

CORRECTIVE ACTION(S)

Criminal Investigation agrees with this recommendation. The Electronic Crimes Management Information System (ECMIS) was intended from the start to be an evidence tracking system that addresses the technically unique and immediate needs of the E-Crimes program. The essential record in the ECMIS database is the item of acquired digital evidence. With the recent transition to direct line management of CISs in E-Crimes, one of the areas of focus for E-Crimes management will be periodic validation of ECMIS data through operational reviews. The requirements for such reviews and other administrative matters are intended to be covered through forthcoming policy directives which are intended to address the technical, security, and legal aspects of the forensics process.

IMPLEMENTATION DATE

COMPLETED Ongoing ____________ PROPOSED 12/31/2008 ________

RESPONSIBLE OFFICIAL

Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN

Director, E-Crimes will ensure that with the newly created direct line management, policy directives are put into place to facilitate the necessary periodic reviews of electronic forensic process.

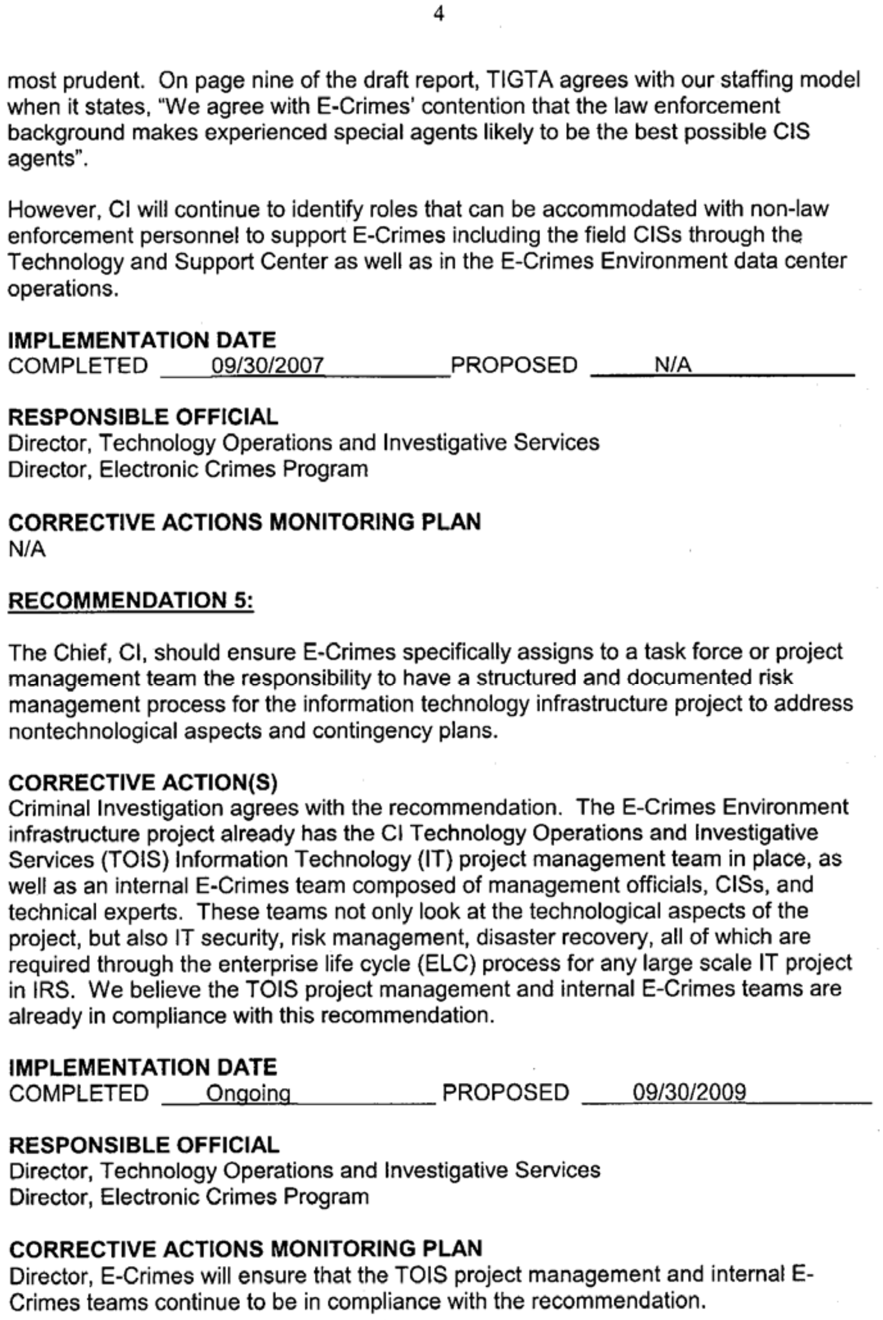
RECOMMENDATION 4:

The Chief, CI, should ensure E-Crimes tests the option of using non-law enforcement positions to benefit the digital evidence field office role.

CORRECTIVE ACTION(S)

Criminal Investigation agrees with the recommendation. We believe that non-law enforcement personnel should be considered where feasible to support or augment the role of a CIS in the field. E-Crimes and CI senior management considered this issue on many occasions throughout the existence of the E-Crimes program. In fact, CI has hired several non-law enforcement technical specialists to support E-Crimes personnel. However, we are unsure how the recommended option can be tested.

Page nine of the draft report suggests CI should consider hiring non-law enforcement personnel to fill some aspects of the CIS role due in part to Special Agent staffing attrition issues. As stated above, CI considered this, but due to the technological, legal, investigative, and financial requirements of the CIS position we continue to believe our current model of having CISs be experienced 1811 Special Agents is the



most prudent. On page nine of the draft report, TIGTA agrees with our staffing model when it states, "We agree with E-Crimes' contention that the law enforcement background makes experienced special agents likely to be the best possible CIS agents".

However, CI will continue to identify roles that can be accommodated with non-law enforcement personnel to support E-Crimes including the field CISs through the Technology and Support Center as well as in the E-Crimes Environment data center operations.

IMPLEMENTATION DATE
COMPLETED 09/30/2007 PROPOSED N/A

RESPONSIBLE OFFICIAL
Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN
N/A

RECOMMENDATION 5:

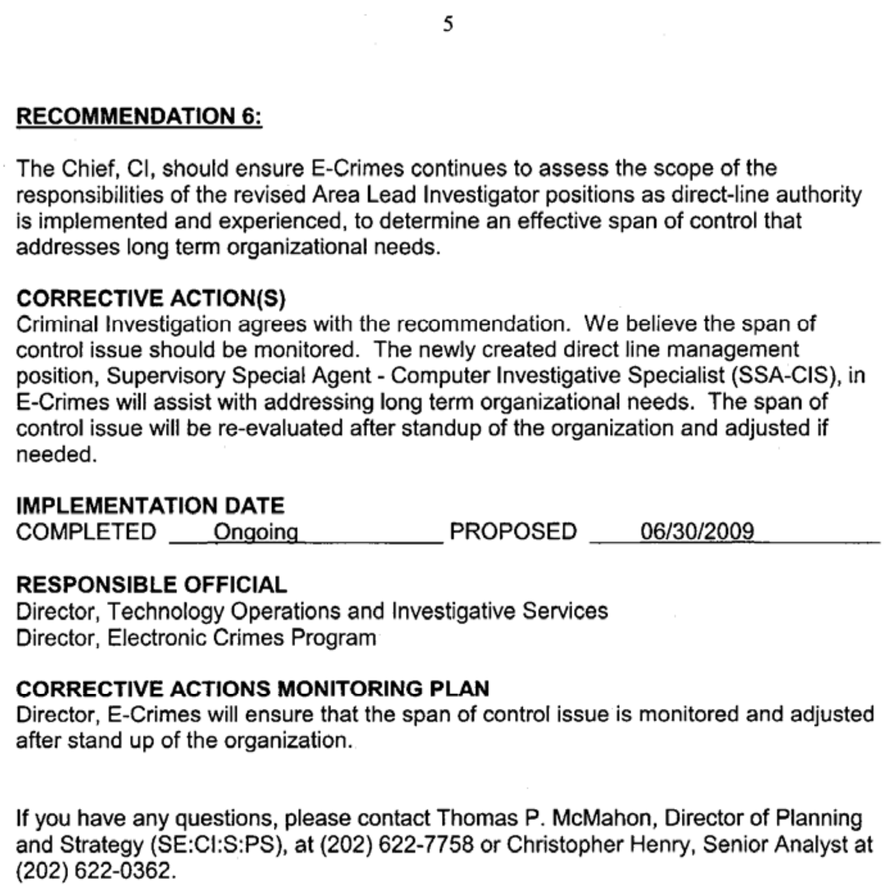
The Chief, CI, should ensure E-Crimes specifically assigns to a task force or project management team the responsibility to have a structured and documented risk management process for the information technology infrastructure project to address nontechnological aspects and contingency plans.

CORRECTIVE ACTION(S)
Criminal Investigation agrees with the recommendation. The E-Crimes Environment infrastructure project already has the CI Technology Operations and Investigative Services (TOIS) Information Technology (IT) project management team in place, as well as an internal E-Crimes team composed of management officials, CISs, and technical experts. These teams not only look at the technological aspects of the project, but also IT security, risk management, disaster recovery, all of which are required through the enterprise life cycle (ELC) process for any large scale IT project in IRS. We believe the TOIS project management and internal E-Crimes teams are already in compliance with this recommendation.

IMPLEMENTATION DATE
COMPLETED Ongoing PROPOSED 09/30/2009

RESPONSIBLE OFFICIAL
Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN
Director, E-Crimes will ensure that the TOIS project management and internal E-Crimes teams continue to be in compliance with the recommendation.



RECOMMENDATION 6:

The Chief, CI, should ensure E-Crimes continues to assess the scope of the responsibilities of the revised Area Lead Investigator positions as direct-line authority is implemented and experienced, to determine an effective span of control that addresses long term organizational needs.

CORRECTIVE ACTION(S)

Criminal Investigation agrees with the recommendation. We believe the span of control issue should be monitored. The newly created direct line management position, Supervisory Special Agent - Computer Investigative Specialist (SSA-CIS), in E-Crimes will assist with addressing long term organizational needs. The span of control issue will be re-evaluated after standup of the organization and adjusted if needed.

IMPLEMENTATION DATE

COMPLETED ____Ongoing____________ PROPOSED ______06/30/2009__________

RESPONSIBLE OFFICIAL

Director, Technology Operations and Investigative Services
Director, Electronic Crimes Program

CORRECTIVE ACTIONS MONITORING PLAN

Director, E-Crimes will ensure that the span of control issue is monitored and adjusted after stand up of the organization.

If you have any questions, please contact Thomas P. McMahon, Director of Planning and Strategy (SE:CI:S:PS), at (202) 622-7758 or Christopher Henry, Senior Analyst at (202) 622-0362.