



# REPORT OF INVESTIGATION



Title (Name and address):  EXEMPT ORGANIZATIONS DATA LOSS		Type of Investigation:  2 - EMPLOYEE INVESTIGATION	Type of Report: <input checked="" type="checkbox"/> Final <input type="checkbox"/> Supplemental
Social Security Number: N/A		<input checked="" type="checkbox"/> Employee <input type="checkbox"/> Non-Employee <input type="checkbox"/> Former Employee	
Date of Birth: N/A	Date Entered on Duty: N/A	Position and Grade: N/A	
Post of Duty: N/A		Division and Office: N/A	
Period of Investigation: June 13, 2014 – June 29, 2015			
Potential Violation(s):  OBSTRUCTION OF JUSTICE			

## INVESTIGATIVE SYNOPSIS

On June 13, 2014, the Treasury Inspector General for Tax Administration (TIGTA) was notified of the computer hard drive failure of Lois LERNER, former Director of the Internal Revenue Service (IRS), Exempt Organizations (EO), Tax Exempt and Government Entities (TE/GE) Division. The hard drive failure was reported by the IRS to have resulted in the loss of LERNER's e-mails, which had previously been requested by Congressional committees, the Department of Justice (DOJ) and TIGTA for their use in ongoing Congressional and criminal investigations of the IRS EO application determination process.

In a letter dated June 23, 2014, the Senate Finance Committee (SFC) requested that TIGTA formally investigate the matter, and that during the investigation TIGTA "perform its own analysis of whether any data can be salvaged and produced to the committee."

Distribution	No.	Case Number:	Signature of Special Agent Making Report:
Inspector General for Tax Administration	1	54-1406-0008-1	[Redacted]
Internal Revenue Service	1	Signature of Person Examining Report:	[Redacted]
Assistant U.S. Attorney	1	[Redacted]	[Redacted]
Other (Specify): House Committee on Ways & Means Committee on Oversight & Government Reform Senate Finance Committee Senate Homeland Security and Governmental Affairs	1 1 1 1	Title: [Redacted] Division Office: SAC, Electronic Crimes and Intelligence Division	Office(City): Washington, DC Date of Report: June 30, 2015

TIGTA Form OI 2028R (Rev 04/2007)

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

On June 23, 2014, the Commissioner of the IRS testified during a hearing before the House Committee on Oversight and Government Reform. During the hearing, additional questions were raised concerning the manner in which the IRS managed and stored LERNER's e-mails.

This investigation was conducted in order to determine if evidence existed that the IRS purposely destroyed or withheld e-mails in an effort to obstruct Congressional and criminal investigations; if any of the e-mails the IRS reported as lost could be recovered; and if the IRS complied with the Federal Records Management Act. The investigation included the interview of 118 witnesses and the review and processing of over 20 terabytes (TB) of data.

The investigation determined that there were six possible sources to examine in order to potentially recover the missing e-mails. These sources were LERNER's crashed hard drive, the backup or disaster recovery tapes, a decommissioned Microsoft (MS) Exchange 2003 e-mail server, the backup tapes for the decommissioned e-mail server, LERNER's BlackBerry, and loaner laptop computers that may have been assigned to her while her laptop was being repaired. An examination of four of these sources, the backup or disaster recovery tapes, the decommissioned Exchange 2003 e-mail server, LERNER's BlackBerry, and the loaner laptops produced e-mail that the IRS had not previously produced to Congress, DOJ or TIGTA. The investigation also determined that once it was discovered that there was a gap in the IRS' production of LERNER's e-mail, the IRS did not fully identify as a source or perform recovery attempts for e-mail on the following electronic media, all of which the IRS had in their possession: backup or disaster recovery tapes, the decommissioned Exchange 2003 e-mail server, the backup tapes for the decommissioned e-mail server or the loaner laptop computers.

As part of the investigative process, TIGTA reviewed and compared data the IRS provided to Congress against datasets independently and forensically obtained by TIGTA. The analysis involved two phases: phase one, a technical comparison; and, phase two, a manual review and comparison of recovered e-mail message body information and associated attachments to the e-mails the IRS produced to Congress. The technical comparison identified over 6,400 e-mails from the backup tapes. In order to determine the entire population of potential e-mails and to look for other useful information, the technical comparison also included the review of IRS e-mail transaction logs involving LERNER's e-mail communications obtained from the Department of the Treasury's (Treasury) Government Security Operations Center (GSOC). The e-mail transaction logs included e-mail communication that was logged as sent *To* or *From* (the log only recorded *To* and *From*, however, the *To* category included courtesy copies and blind courtesy copies) LERNER from February 1, 2010 through May 7, 2013. The message header information from these logs was compared to what the IRS had previously provided to Congress. The result of the comparison indicated that as many as 23,000 to 24,000 e-mail messages may not have been provided to Congress. As the logs contained message headers only, the body and attachments related to these e-mail messages were not present, and therefore, not recovered from any data sources gathered

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 2

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

during this investigation. A manual comparison of the IRS e-mail transition logs to the IRS production to Congress was not possible, as these logs did not contain any message body or attachments, and therefore, the 23,000 to 24,000 estimate could be high.

In the second phase, TIGTA special agents (SAs) conducted a manual review of the aforementioned e-mail sources and identified 1,330 e-mails from the four sources that the IRS did not produce to Congress, the DOJ or to TIGTA.

The investigation also revealed that on or about March 4, 2014, one month after the IRS realized it was missing some of LERNER's e-mails, IRS employees in the IRS Enterprise Computing Center in Martinsburg, West Virginia (Martinsburg), magnetically erased 422 backup tapes that are believed to have contained LERNER's e-mails that were responsive to Congressional demands and subpoenas. However, the investigation did not uncover evidence that the IRS and its employees purposely erased the tapes in order to conceal responsive e-mails from the Congress, the DOJ and TIGTA.

The investigation revealed that the backup tapes were destroyed as a result of IRS management failing to ensure that a May 22, 2013, e-mail directive from the IRS Chief Technology Officer (CTO) concerning the preservation of electronic e-mail media was fully understood and followed by all of the IRS employees responsible for handling and disposing of e-mail backup media. In December 2011, IRS Information Technology (IT) employees in the IRS New Carrollton Federal Building (NCFB) disassembled the Exchange 2003 Server, as well as many other servers in the same room, and they treated the decommissioned server hard drives and backup tapes like junk, moving them from room to room in the NCFB until they could be shipped out for destruction. In April 2012, the majority, but not all, of the equipment from the decommissioned server room was destroyed by IRS contractor UNICOR. In December 2013, the IRS was preparing to renovate the room at the NCFB where the remaining Exchange 2003 components were stored. In order to clean out the room, the order was given to ship the server components and backup tapes to Martinsburg for destruction. On January 29, 2014, the server components and backup tapes were loaded on a truck and shipped to Martinsburg. The proper paperwork (Form 3210) did not accompany the shipment, so the employees at Martinsburg left the shipment untouched until March 4, 2014, when [REDACTED], the IRS IT Specialist [REDACTED], sent the Form 3210 to ECC-MTB. Upon receipt of the Form 3210, the midnight shift employees at Martinsburg degaussed (magnetically erased) the backup tapes. The employees did not degauss the server hard drives that were shipped with the backup tapes because their interpretation of the CTO's May 22, 2013, e-mail directive was that it was meant to preserve hard drives only. This misinterpretation resulted in the continued destruction of tape media until June 2014, when management realized the misinterpretation and put a halt to the destruction of all of the tape media. Although they existed until March 4, 2014, the backup tapes containing LERNER's e-mails were destroyed because the IRS employees who shipped the backup tapes and server hard drives did not understand their responsibility to comply with the CTO's May

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

---

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 3

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



## REPORT OF INVESTIGATION

2013 e-mail directive to preserve electronic backup media and the Martinsburg employees who destroyed the backup tapes on March 4, 2014, misinterpreted the directive.

In addition to interviewing the line and management employees involved in the processing of the e-mail backup tapes, the investigation included interviews of IRS Senior Executives, including The Honorable John KOSKINEN, IRS Commissioner, Terence MILHOLLAND, IRS CTO, and Stephen MANNING, former IRS Deputy Chief Information Officer, Strategy and Modernization.

When interviewed, MANNING stated that he was responsible for providing technical explanations to IRS senior management and Chief Counsel, as well as coordinating the internal flow of data from IRS IT personnel during the process of gathering data for the IRS' production process to Congress for the IRS EO matter. MANNING related that although the issue of e-mail backup tapes came up almost immediately in May 2013, specifically with respect to how far back the IRS maintained them, no e-mail was restored from backup tapes because nothing had been determined to be missing at that time. MANNING added that after the discovery that LERNER's hard drive had failed, a "second wave" of e-mail backup related questions came in during February or March 2014. MANNING stated that the decisions on whether or not to restore data from tape backups rested with IRS Chief Counsel, but it was not considered because the tape backups only went back to November 2012, which was significantly after LERNER's hard drive failure in 2011. MANNING admitted that the Exchange 2003 Server infrastructure retired in 2011, would still have been covered under the May 2013, CTO e-mail directive requiring e-mail accounts be preserved.

On May 22, 2013, MILHOLLAND issued a policy directive via e-mail that was titled "Information Retention Policy Revision," changing the backup tape recycle policy from six months to an indefinite retention period for all e-mail backup tapes. In this policy directive, MILHOLLAND also ordered that "Given the current environment and ongoing investigations, until further notice, do not destroy/wipe/reuse any of the existing backup tapes for email, or archiving of other information from IRS personal computers. Further, do not reuse or refresh or wipe information from any personal computer that is being reclaimed/returned/refreshed/updated from any employee or contractor of the IRS." MILHOLLAND added, "In other words, retain everything to do with email or information that may have been stored locally on a personal computer."

When interviewed, MILHOLLAND was asked if he knew that e-mail backup tapes from a decommissioned e-mail server had been degaussed in March 2014. MILHOLLAND stated that he was not aware of this, and he advised that he was "blown away" at the revelation. He further stated that IRS IT senior management was ultimately responsible. MILHOLLAND also stated that his May 2013 e-mail directive would have applied to preserving the NCFB backup tapes and that the organization that sent them to be destroyed would also be responsible for their destruction.

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 4

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

When interviewed, Mr. KOSKINEN testified he was briefed by his senior advisors about the data loss and the "disaster recovery" tapes. Based on his briefing, he was under the impression that retrieving LERNER's missing e-mails from these tapes would not be feasible. Mr. KOSKINEN said he was not aware that the 422 backup tapes that most likely contained missing LERNER e-mails had been erased on March 4, 2014. Mr. KOSKINEN added that he believed that the investigation would play an important role and will be helpful in determining what the IRS can do to improve its processes. Mr. KOSKINEN stated that when he learned of the missing e-mails and that there was a gap in the production, he provided the idea to search the additional 83 custodians for LERNER e-mails in an effort to locate all of the pertinent e-mails. He also stated he was not directed to destroy, nor did he direct the destruction of any e-mails. Mr. KOSKINEN stated that he advised his staff to cooperate fully in the investigation and that obtaining any missing e-mails would be important.

The investigative synopsis is separated into four primary categories:

**LERNER Hard Drive Failure:** Details the identification and the apparent ultimate resolution of LERNER's failed computer hard drive.

**Additional Custodian Hard Drive Failures:** Details the hard drive failures of other IRS employees who may have sent or received e-mails pertinent to the IRS EO Determinations process.

**Other Potential Sources of E-mail Messages:** Details the efforts to identify, obtain, and analyze IRS MS Exchange server drives, backup tapes, IRS loaner laptops, LERNER's BlackBerry, Offsite Contractor Storage of Backup Tapes, and Network Transaction Logs.

**Federal Records Management Act Compliance:** Details the IRS' use and records retention of MS Office Communicator Server (OCS) and the "instant messaging" function of OCS; and, describes the IRS' compliance with the applicable IRS/National Archives and Records Administration policies for defining records and explains records retention requirements.

### LERNER Hard Drive Failure

On June 13, 2011, IRS Information Technology Asset Management System (ITAMS) ticket number 8455435 was entered indicating LERNER's "computer screen is black and won't allow [the] employee to log in." IRS employee [REDACTED], an IT Specialist, was identified as the IRS employee assigned to respond to LERNER's ticket. [REDACTED] was interviewed under oath and he confirmed he responded to the June 13, 2011, helpdesk ticket associated with LERNER's failed hard drive. [REDACTED] explained he was unable to recover any data from the hard drive, and following normal protocol, he replaced the hard drive in LERNER's computer with a new hard drive. [REDACTED] placed the damaged hard drive in a box with other damaged electronics awaiting to be destroyed. An ITAMS helpdesk ticket indicated that upon replacing the drive, [REDACTED] determined that LERNER's laptop

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 5

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

needed a new system fan and possibly a heatsink due to overheating. Therefore, a request was made for technical support from Hewlett-Packard (HP).

██████████ stated that he did not observe any indications of tampering or physical damage to LERNER's laptop.

The investigation identified ██████████, a Computer Technician for Managed Print Services, ██████████ as the outside expert who worked on LERNER's laptop to replace the keyboard, trackpad, heat sink, and fan due to an overheating issue per the ITAMS ticket input by ██████████. ██████████ was interviewed regarding his observations of the status of LERNER's laptop. ██████████ opined it was unusual for so many components to fail at the same time, but did not recall, or note in his records, any damage to the laptop. Had any damage been observed, ██████████ advised another ticket would have been initiated to repair any newly identified problems. ██████████ stated that many different things, including the environment, could cause damage to a computer. From his experience, keyboards and trackpads are usually damaged by liquid spilling on them, although this was not observed in this specific incident. Excessive heat can cause damage to a hard drive and it also depends whether the hard drive is located under the laptop or on the side; hard drives located under the laptop tend to overheat more easily. ██████████ related that there are many causes for hard drive failures, although overheating causing a hard drive failure is not often seen. If there was severe impact to a computer or hard drive, it could internally damage the mechanical components of the hard drive making it unusable. When asked what scenario could have caused hard drive heads to impact the platter of the disk, ██████████ opined an impact to the laptop or hard drive was the most likely cause.

This investigation was unable to confirm specific tracking of LERNER's failed hard drive because the IRS only tracked laptops and computers as singular entities, and did not track components, such as hard drives by serial numbers. The location and possession of LERNER's failed hard drive was established via reviews of documents, interviews, and the review of e-mail conversations between IRS employees.

Following normal protocol, ██████████ stored LERNER's failed hard drive with other failed IRS hard drives until ██████████ was contacted by IRS Program Manager ██████████. ██████████ advised she was contacted by former IRS Associate Chief Information Officer, ██████████ who asked her to make an effort at recovering information off LERNER's hard drive because LERNER had made a special request claiming the hard drive contained LERNER's personal files.

On July 20, 2011, ██████████ directed ██████████ to ship the hard drive out for a more extensive data recovery effort. Following ██████████'s instructions, ██████████ retrieved the hard drive he believed to be LERNER's and he sent it, in ██████████'s name to the IRS Washington, DC IT Depot located at 1111 Constitution Avenue, NW, Washington, DC. Subsequently, LERNER's failed hard drive was

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-1

TIGTA Form OI 2028R (Rev. 04/2007)

Page 6

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



## REPORT OF INVESTIGATION

hand delivered to [REDACTED], Senior Analyst, IRS-Criminal Investigation Division (IRS-CI), in Alexandria, Virginia.

When interviewed, [REDACTED] stated he received LERNER's hard drive on July 22, 2011, and attempted to recover data from it but was unsuccessful despite using diagnostic tools and substituting known good parts from two donor hard drives. [REDACTED] noted concentric scoring of the hard drive platters, opining that the drive had failed because the drive heads had impacted the platters while in operation ([REDACTED] did not photograph the damage). [REDACTED] returned LERNER's failed hard drive to the IRS Washington, DC, IT Depot on August 5, 2011, and advised data could still potentially be recovered using a third donor hard drive or hiring an outside vendor. [REDACTED] confirmed data may have been recoverable by an outside vendor, but she ([REDACTED]) decided the expense was not justified due to financial constraints, as well as the fact that LERNER had categorized the data present on the drive as being personal in nature.

The hard drive believed to be LERNER's failed drive was signed for and received on August 8, 2011, by IRS Program Analyst [REDACTED] in Washington, DC. An interview with [REDACTED] revealed he could not recall specifically the delivery of the hard drive, but advised he would have followed standard procedure for a failed hard drive, which involved placing it in a container with other failed hard drives to begin the process to being excessed and destroyed. Once the boxes of failed hard drives and other equipment become full at the IT Depot, the boxes are shipped to NCFB to be picked up for destruction by a vendor.

The Federal Prison Industries, Incorporated, (also known as UNICOR) is a Federal Bureau of Prisons, DOJ program that was operating under a Memorandum of Understanding (MOU) with the IRS to destroy electronic media, and periodically picked up failed media from the Washington, DC area at the NCFB. The next known UNICOR pickup after August 2011 (the last reference available to the location of LERNER's failed hard drive) was April 13, 2012. According to a "Department of Justice, UNICOR, Certificate of Destruction" dated April 16, 2012, this shipment, which contained "hard drives" and other computer equipment (believed to include LERNER's failed hard drive) was destroyed at the UNICOR Recycling Facility in Marianna, FL, on April 16, 2012.

[REDACTED] of the UNICOR Recycling Facility in Marianna, FL, provided the MOU between the IRS (customer) and UNICOR dated September 27, 2007. The MOU states in order to prevent the disclosure of data, all hard drives, flash drives, tape drives, magnetic tapes, floppy disks, compact disks, and other electronic media storage components containing sensitive data received from the IRS must be obliterated, not reconditioned and reassigned, by UNICOR. [REDACTED] was provided the hard drive serial number for LERNER's failed hard drive to determine if UNICOR had any record of the hard drive. [REDACTED] advised that under the MOU with the IRS, UNICOR did not track the IRS drives by serial number, so he had no specific record of the hard drive. [REDACTED] also explained that his staff disposes of the shipments shortly after arriving. [REDACTED] identified the AMERI-

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-1

TIGTA Form OI 2028R (Rev. 04/2007)

Page 7

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

SHRED AMS-750HD, Serial Number 2308103-A, as the only hard drive shredder the UNICOR Recycling Facility has that would have been used to shred the 300 pounds of hard drives received from the IRS on April 16, 2012. TIGTA SAs viewed the remnants of hard drives that were processed through this shredder. The end-result of the shredding process is that pieces are cut into quarter-sized pieces that are then sold as scrap.

On July 29, 2014, TIGTA SAs inspected the UNICOR Recycling Facility and looked for any hard drives that were not destroyed. The inspection revealed that when shipments are received they are moved and destroyed. There was no holding area or bin of older shipments awaiting destruction.

Given that LERNER's laptop hard drive was more than likely destroyed and was not available for forensic inspection and examination for this investigation, no definitive, first hand conclusion could be reached regarding the cause of the LERNER's laptop hard drive failure.

TIGTA secured LERNER's assigned IRS laptop from the IRS on June 10, 2013. LERNER's laptop, which was placed into TIGTA evidence, was photographed by the TIGTA Forensic Science Lab to document its condition. There were no obvious signs of external damage noted, although several screws on the underside appeared to show signs of wear, consistent with what would occur when removing and replacing a hard drive or other internal components.

Analysis of available IRS network logs associated with LERNER's laptop was undertaken to determine the status of the laptop immediately prior to the hard drive failure. The IRS employs a custom network query tool to gather information from devices connected to the IRS network in two-hour intervals. A review of these historical network logs indicated LERNER's laptop containing the failed hard drive was powered on and connected to the IRS network almost non-stop between May 31 and June 11, 2011, with few exceptions reflected in missed query responses. These logs also revealed the laptop was assigned an Internet Protocol (IP) address, which could only have been assigned to a device residing inside an IRS facility for the entire period of May 31 through June 11, 2011. This was consistent with information provided by [REDACTED], LERNER's Staff Assistant who advised LERNER almost never took her laptop home or on travel.

The last query LERNER's laptop responded to before it was reportedly discovered on June 13, 2011, as having a failed hard drive, was on Saturday, June 11, 2011, at 5 PM Eastern Daylight Time (EDT). The laptop failed to respond to the subsequent network query at 7 PM EDT and every other query between June 11 and June 20, 2011, at which time the laptop had been repaired; a new hard drive installed, and the laptop was returned to LERNER.

A forensic analysis of LERNER's laptop revealed the first log in of the newly installed MS Windows Operating System was in fact near the date and time detected in the network query tool logs on June

---

Case Title: EXEMPT ORGANIZATIONS DATA LOSS	Case Number: 54-1406-0008-I
---	--------------------------------

TIGTA Form OI 2028R (Rev. 04/2007)

Page 8

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



---

## REPORT OF INVESTIGATION

---

20, 2011, validating that this was the first time LERNER's laptop had been connected to the IRS network.

The lack of responses after 5 PM EDT, June 11, 2011, could have been caused by a number of factors, the most likely of which being that, the hard drive failed, that it was disconnected from the network, or that a network disruption interfered with the query being sent or received. At TIGTA's request, the IRS Computer Security Incident Response Center (CSIRC) researched the network segment for LERNER's laptop connection and the network query tool for any signs of irregular activity, or lack of activity during the period LERNER's laptop failed to respond. CSIRC advised the network query tool was functioning normally and was receiving responses from other computers on the same network segment as LERNER's laptop, indicating the lack of responses was not likely due to a network problem, or a network query tool problem.

A review of available IRS logs detailing new software sent to client machines on or about June 11, 2011, revealed LERNER's laptop was one of 359 IRS computers that were scheduled to receive an "uninstall" software package, which was being phased out on many clients across the IRS network. The delivery window for the software package was between June 8 and June 11, 2011, at 3:57 PM EDT. Interviews of IRS employees familiar with the process stated the electronic package delivery, which the logs indicated was "successful" with respect to LERNER's laptop, would have likely occurred as soon as the client machines were connected to the network during the window. Based on the fact that LERNER's laptop was communicating on the network on June 8, 2011, it is probable the software package was delivered on that date. It is also possible, however, that this software uninstall occurred as late as 3:57 PM EDT, June 11, 2011, which was one hour prior to the last documented network communication from LERNER's laptop. As background, Hummingbird Exceed was utilized to facilitate secure data communications between client systems and specialized IRS servers. There is no indication that the software uninstall would have caused LERNER's hard drive to crash.

In order to determine if anyone entered LERNER's office prior to the hard drive crash to tamper with or remove the laptop, attempts were made to recover security badge entry and exit logs to 1750 Pennsylvania Avenue NW, Washington DC, which housed LERNER's office at the time. TIGTA was informed by Kastle Systems, the security company responsible for maintaining the logs, that those logs were no longer available, as they were only kept for one year. A site survey of the building revealed there were no other systems or monitoring platforms that would have captured anyone entering or exiting the building in June 2011. During this investigation, it was also determined the EO Division no longer occupies office space at the 1750 Pennsylvania Avenue location, as the EO Division moved from this location in approximately December 2011.

LERNER was interviewed regarding the circumstances of, and data loss from, her failed laptop hard drive. LERNER described herself as having "rudimentary" knowledge with respect to computers.

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

---

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 9

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

She advised she knew the basic operations for the use of MS Outlook, the e-mail client used by the IRS. When asked how she normally processed her IRS e-mail, LERNER advised she received 100 to 200 e-mails each day and frequently was unable to review all messages she received. She moved e-mail to various compartmentalized "folders" on her laptop representing different topics or programs in the left panel of MS Outlook. LERNER has "no idea" regarding the quantity of file folders, but it was "more not less." LERNER did not know how Personal Storage Table (PST) files containing her e-mail would have been created on her local hard drive. LERNER stated her IRS e-mail account had a limit to the amount of e-mail it would hold. When the limit was reached, she would be unable to send additional e-mail. To resolve the issue, she went to the oldest e-mails and deleted them. LERNER did screen her e-mail to determine if each e-mail may be important before deleting the e-mail.

LERNER remembered her hard drive failure in June 2011, which resulted in a significant amount of data being lost. She described coming into office in the morning and seeing "the blue screen." LERNER advised there had been no previous problems with the hard drive. Someone, whom LERNER could not recall, told her the hard drive had failed, but that they might be able to recover the data. Although LERNER believed this additional attempt to recover data did cost an additional fee, she believed the work would be performed within the IRS and would be a worthwhile use of funds because all of her work files were contained on the hard drive. LERNER recalled that this hard drive failure cost her "a lot of time" because so much of her current work was lost. LERNER was "surprised" that IRS IT could not do more to recover her e-mail. LERNER did not recall how long IRS IT waited to inform her that her data was not recoverable or specifically what steps or tools IRS IT staff used in order to recover the data. LERNER denied hitting or damaging the hard drive intentionally. LERNER stated that she typically left her laptop inside of her locked office for fear that it may be stolen. LERNER did not recall any incidents that could have damaged her laptop. LERNER was not aware of anyone who might want to destroy the data on her computer.

Thomas KANE, Deputy Associate Chief Counsel, IRS, Office of Chief Counsel, Procedure and Administration (P&A), Washington, DC, was interviewed under oath. KANE stated that on February 4, 2014, the IRS Office of Chief Counsel, with assistance from IRS IT, determined LERNER experienced a hard drive failure on June 13, 2011; the hard drive failure was documented by IRS IT helpdesk tickets and e-mail messages dated June 13, 2011. LERNER's hard drive failure was discovered after reviewing a list of LERNER e-mails already produced to Congressional committees, and it was noted she had substantially more e-mails after 2011. KANE further stated the decision was made to wait and develop the most complete and accurate picture before officially making notification to Congress; this was the genesis of a "white paper" document generated by the IRS and dated June 13, 2014, addressed to the SFC, which served as notification to Congress regarding LERNER's failed hard drive. According to KANE, Mr. KOSKINEN wanted to finish the production of LERNER e-mails and produce all of the LERNER e-mails with an explanation for the missing e-mails. The intention was to release the "white paper" when the production of all the LERNER e-mails was

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-1

TIGTA Form OI 2028R (Rev. 04/2007)

Page 10

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

complete, which was anticipated at the end of June 2014. The "white paper" was released early, and prior to the completion of the LERNER e-mail production, because two Congressional committees anticipated releasing their reports in June 2014 and wanted a full explanation of what e-mails had already been produced and what was still expected.

KANE also stated Catherine DUVAL, former Counselor to the Commissioner, IRS, Office of Chief Counsel, Washington, DC, was the IRS point of contact for the Treasury Office of General Counsel (OGC) and likely had regularly scheduled meetings with Treasury. DUVAL briefed [REDACTED], Attorney, Treasury OGC, Washington, DC, regarding the issue with the LERNER e-mails. KANE explained that the IRS is justified in advising the Treasury OGC about the production of records since the IRS is subordinate to the Treasury and because Congress issued subpoenas to Treasury Secretary Jacob LEW, requesting IRS e-mails and documents effectively holding him and Treasury responsible for the responsive documents, including LERNER's e-mails.

When interviewed, DUVAL stated that she was working with IRS Counsel on the production when they noticed they were missing e-mails. DUVAL stated that the focus was on trying to recover the missing e-mails from the other custodians who sent or received e-mails from LERNER. DUVAL stated the team was also trying to determine if any of the custodians had also suffered data losses. In approximately April 2014, she briefed the Treasury OGC and advised the OGC that the IRS was looking into an issue regarding LERNER's missing e-mails.

### Additional Custodian Hard Drive Failures

On June 23, 2014, the SFC requested TIGTA determine if IRS employees LERNER, Nikole FLAX, [REDACTED], [REDACTED], [REDACTED], and [REDACTED], experienced a data loss because of hard drive failures. On June 16, 2014, the IRS provided these names to the SFC and other Congressional committees as individuals with potential hard drive failures and data loss.

In addition to the aforementioned June 23, 2014, request, the SFC presented TIGTA with a list of names of 119 IRS employees (which included the seven names listed in the prior paragraph) and requested that TIGTA determine if any of the 119 IRS employees experienced a hard drive failure and subsequent data loss. Through a review of IRS helpdesk tickets, and interviews of the IRS employees themselves and IRS IT Specialists, TIGTA concluded that IRS employees [REDACTED], [REDACTED], [REDACTED], [REDACTED], and [REDACTED] experienced a data loss because of hard drive failures. TIGTA was also able to conclude that although Nikole FLAX, [REDACTED], [REDACTED], and [REDACTED] experienced hard drive failures, they did not experience a data loss. Also included on the list of 119 IRS employees, [REDACTED] was identified as having data loss only; IRS IT believed the data loss was the result of an operating system/software error, and was not a hard drive issue. IRS IT

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

---

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 11

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



## REPORT OF INVESTIGATION

generally did not have information concerning the specific hard drive failure incidents, but explained that the steps typically taken in an effort to recover data from a hard drive included running a diagnostic test and attempting to run the hard drive in a separate computer. IRS IT further explained there were no additional steps or resources available to recover data from the hard drives.

A review of IRS helpdesk tickets also identified [REDACTED], Program Manager, IRS, EO, TE/GE, [REDACTED] as having experienced a hard drive failure. When interviewed, [REDACTED] stated his hard drive failure occurred in September 2013 and his computer data was previously copied in June 2013, therefore, any data lost on the computer was previously copied and retained by IRS IT. IRS IT confirmed the imaging of [REDACTED] computer in June 2013.

TIGTA did not identify a data loss associated with former IRS Tax Law Specialist [REDACTED] because [REDACTED] was interviewed by TIGTA and stated he did not recall a data loss. The IRS was not aware of the data loss which TIGTA identified associated with [REDACTED] [REDACTED] [REDACTED] or [REDACTED] because the IRS only researched potential hard drive failures associated with the 82 custodians that represent the IRS employees identified with e-mails and documents (relevant to IRS EO Determinations) which were produced to Congressional committees. However, TIGTA researched potential hard drive failures associated with the individuals included on the list of 119 IRS employees presented by the SFC and [REDACTED] [REDACTED] [REDACTED] and [REDACTED] were not on the list of 82 custodians. None of their e-mail was provided to Congress and any data loss would not have relevance to Congressional committees. The list of 119 names was generated by the IRS and provided to Congressional committees, but it was ultimately reduced to 82 custodians. The list of 119 names in the request from the SFC includes IRS employees with no relevance to or impact on the Congressional investigations.

The failed hard drives for three of the custodians identified in this investigation, including [REDACTED] [REDACTED] and [REDACTED], who had posts of duty in Ohio, would have been sent to Martinsburg for destruction. Per a Certificate of Destruction dated May 7, 2012, an outside vendor destroyed 211,586 pieces of media, which most likely contained [REDACTED] hard drive as his hard drive failed on September 9, 2011. TIGTA was able to locate and take possession of [REDACTED]'s failed hard drive, but was unable to recover any information from the drive using standard forensic tools. TIGTA will contract with a vendor to determine if in fact any information can ultimately be recovered. The remaining custodian hard drive failures occurred after May 7, 2012.

### Other Potential Sources of E-mail Messages

The IRS utilizes MS Exchange to provide enterprise e-mail accounts to employees. IRS IT reported that backups are performed incrementally on a daily basis (meaning only changes since the last incremental backup are recorded), while a full backup is performed weekly of all MS Exchange Server databases. On average, the IRS uses 27 tapes per week for full backups and four tapes per day for

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 12

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

incremental backups. Up until April 2013, the IRS was reusing and recycling (putting tapes back into circulation to be written over with new backup data) backup tapes every six months as a cost saving measure.

This process was changed on May 22, 2013, when the CTO issued a policy directive via e-mail titled "Information Retention Policy Revision," changing the backup tape recycle policy to an indefinite retention period for all e-mail backup tapes. In this policy directive, the CTO also ordered that "Given the current environment and ongoing investigations, until further notice, do not destroy/wipe/reuse any of the existing backup tapes for email, or archiving of other information from IRS personal computers. Further, do not reuse or refresh or wipe information from any personal computer that is being reclaimed/returned/refreshed/updated from any employee or contractor of the IRS" and "In other words, retain everything to do with email or information that may have been stored locally on a personal computer."

Interviews of IRS IT personnel revealed that LERNER's e-mail account would have been housed on Exchange Servers located at two different locations during the period-of-time in question; first at NCFB, then at Martinsburg. On or around May 2011, the IRS e-mail server at NCFB was migrated from an Exchange 2003 Server to a new Exchange 2010 Server at Martinsburg. The migration was part of an IRS effort to consolidate from 11 e-mail data centers down to three, as a part of the Treasury driven Federal Data Center Consolidation Initiative (FDCCI), and was an attempt to enhance the stability of IRS e-mail servers. The server room at the NCFB was repurposed in accordance with the FDCCI, into an Enterprise Networks Command Center, which was approved on June 22, 2011.

The NCFB Exchange 2003 Server was connected to a large Storage Area Network (SAN) array collectively made up of hundreds of hard drives. When the NCFB Exchange 2003 Server was taken out of service, it was left in place because approximately 12 other servers were connected to the same SAN. Due to the shared architecture, those servers had to be decommissioned before the Exchange 2003 Server could be disassembled. Interviews and e-mail analysis indicate the NCFB Exchange 2003 Server was likely disassembled in the spring of 2012. Initial reporting to TIGTA regarding the status of this MS Exchange Server indicated "the legacy tape drives and all associated old equipment in NCFB were destroyed."

### ***Active Microsoft Exchange Server Backup Tapes***

As a result of the June 30, 2014, demand made by TIGTA for any backup tapes that would contain LERNER's e-mails from January 1, 2008, through December 31, 2011, the IRS Data Management Support and Services (DMSS) staff identified 744 tapes, which may have been utilized to back up the Exchange Server which contained LERNER's e-mail account. These tapes were identified based on queries of an electronic tape archive that tracked backup tapes actively in use by the IRS. TIGTA

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-1

TIGTA Form OI 2028R (Rev. 04/2007)

Page 13

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

took possession of these tapes on July 1, 2014. During a subsequent review of tape archive information related to those tapes, DMSS identified a subset of 13 tapes which were believed to contain five sets of weekly backups beginning on November 20, 2012. These tapes constituted the oldest known LERNER e-mail account backups available at the time. At the time these tapes were identified, DMSS indicated it was "likely" the backup tapes from the NCFB Exchange 2003 Server decommissioned in 2011, "would have been destroyed or recycled" and that they were "collecting the appropriate documents to prove that the formal procedures were followed with appropriate approval for the destruction of tapes," indicating an update would follow.

During the process of identifying and recovering the 744 tapes, DMSS identified nine tapes in the automated e-mail archiving infrastructure known as the "robot" which they did not expect to find because they did not have a corresponding record in the electronic index responsible for tracking the tapes. These tapes were believed to be "expired in November of 2012," meaning they would have been marked for re-use under the policy in effect in November 2012. At the time they were provided, DMSS could not say when the last time these nine tapes had actually been written to, but it was possible they could contain the oldest copy of LERNER's e-mails. Due to the age of the technology and the uniqueness of the backup tapes, TIGTA provided these nine tapes to the Federal Bureau of Investigation (FBI) for forensic analysis. The FBI analysis revealed the nine backup tapes contained no logical information. A secondary analysis by Kroll Ontrack (Kroll), a well-established, third-party data recovery service provider, also revealed the nine tapes contained no logical (active) or forensically retrievable information. [REDACTED], IT Specialist, IRS, Enterprise Operations (EOPS), DMSS, advised this finding was not entirely unexpected, as these nine tapes had likely been identified as "scratch," or bad, by the system, and thus, were likely never written to by the tape robot.

Recovery and extraction of the data residing on the 13 backup tapes by Kroll yielded nearly 15.1 TB of data consisting of approximately 83 million e-mail messages in addition to five MS Exchange database files containing five incremental backups of LERNER's e-mail boxes. The five e-mail boxes yielded approximately 80,000 e-mail messages, which, after removing duplicates, yielded approximately 32,000 e-mail messages, which ranged from the years 2001 to 2013. Due to the manner in which the IRS produced information to Congress, off-the-shelf software was not useful in conducting the comparison of the e-mails that TIGTA recovered to the e-mails the IRS had already provided to the Congress. Custom scripting compiled by TIGTA's Electronic Crimes and Intelligence Division personnel yielded the identification of approximately 6,400 e-mail items, which may not have been previously provided by the IRS to Congress. This custom program based these comparisons on technical features of the e-mail themselves, and did not make a judgment on the relative newness of the concepts relayed by their authors.

To assist in the expeditious completion of the various ongoing investigations being conducted by committees of the Congress, the DOJ and TIGTA, the 6,400 e-mails were provided to the requesting Congressional committees of Congress with authority to receive them, to DOJ, and to the IRS.

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

---

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 14

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



## REPORT OF INVESTIGATION

TIGTA reviewed all of the e-mails for information or evidence that may be pertinent to the investigation. In addition, TIGTA manually reviewed all of the e-mails and determined that after individual manual inspection and the removal of spam e-mails, approximately 1,007 e-mails were actually new e-mails that were not previously provided by the IRS to the Congress, DOJ or to TIGTA. It must be noted that TIGTA is in the process of separately reviewing the entire 15.1 TB of data again to ensure all of the pertinent e-mails have been identified. This process will take as many as two additional months to complete. However, if new e-mails or information is identified, the new e-mails will be evaluated, a supplemental report will be written, and the new material will be provided to the investigating committees, the DOJ and the IRS.

### ***Decommissioned Microsoft Exchange Server Hard Drives and Associated Backup Tapes***

Continuing the search for backup tapes and hard drives, on July 11, 2014, a [REDACTED] manager advised TIGTA that they had identified 760 hard drives, which they believed, were part of the decommissioned Exchange 2003 e-mail server from NCFB. These drives had been located in a storage facility at Martinsburg and had not been destroyed as previously thought, however, [REDACTED] stated they believed the data on the hard drives would have been overwritten (in order to make data on them unrecoverable) prior to their shipment from the NCFB to Martinsburg per the standard procedure. There are discrepancies in IRS employee testimony and documentation concerning the actual number of hard drives. The Document Transmittal (Form 3210) that was associated with the server drives from the NCFB reported the number of drives as 300. [REDACTED], IRS Supervisory Computer Assistant, the responsible [REDACTED] onsite manager, reported that he personally counted 764 hard drives; two additional employees were directed to count the hard drives and reported their counts as 850 hard drives. This discrepancy remains of investigative interest, and is still under investigation. On July 11, 2014, TIGTA took possession of the 760 hard drives identified and provided by [REDACTED], subsequently placing them into evidence. During the exchange of information regarding these hard drives, [REDACTED] stated that the backup tapes associated with this server had been degaussed. The IRS defines the process of degaussing in accordance with the Internal Revenue Manual (IRM) section 2.7.4.5.4, Degaussing Methodology Summary, which states the following:

*An alternating current (AC) bulk eraser (degausser) is used for complete erasure of data and other signals on magnetic media. Degaussing is a process where magnetic media is exposed to a powerful, alternating magnetic field. Degaussing removes any previously written data, leaving the media in a magnetically randomized (blank) state. The degausser must subject the media to an alternating magnetic field of sufficient intensity to saturate the media and then by slowly withdrawing or reducing the field, the magnetic media is left in a magnetically neutral state.*

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 15

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

Over the course of the investigation, interviews routinely revealed that the IRS did not have a process that tracked individual hard drives that had been removed from a computer or server. Follow-up interviews with IRS EOPS personnel were conducted in February 2015, to determine what process was used by the IRS to track the 760 hard drives from the Exchange 2003 Server that was decommissioned at NCFB in May 2011, to Martinsburg, where, pursuant to the TIGTA demand for media they were found on July 11, 2014. IRS EOPS Media Management Midnight Unit personnel, were aware of the hard drives only because they had arrived on an unexpected shipment on January 29, 2014, and the disposition took several months to resolve. The hard drives were not degaussed upon receipt at Martinsburg because the Form 3210, which is required to destroy the media, was not present with the shipment. A copy of the Form 3210 was obtained by TIGTA on February 13, 2015, from IRS Supervisory Program Manager [REDACTED] which indicated it had been completed and signed by the requestor, [REDACTED] on March 4, 2014. Along with the 300 hard drives, the Form 3210 also listed "600 NEW in the box LTO tape media" and "600 LTO backup tape media – PII."

[REDACTED] staff and [REDACTED] were questioned about the presence of 300 backup tapes containing "PII" with the shipment to Martinsburg, which were subsequently described as an approximate count of tapes used to back up the decommissioned NCFB Exchange 2003 Server, as well as IRS user network storage. The count was approximate because [REDACTED] filled it out in March 2014, several months after the shipment had been loaded onto pallets, and he could not recall specific numbers. The existence of these hard drives came to the attention of TIGTA because, in response to TIGTA's demand for tapes on June 30, 2014, [REDACTED] had been asked by DMSS to look into this shipment and determine if the tapes had been degaussed. [REDACTED] subsequently advised [REDACTED] that the hard drives in the shipment were likely from a server array and may have been related to the backup tapes.

Martinsburg is one of three centers designated by the IRS as an acceptable alternate destruction site for IRS locations that are not able to destroy media themselves. Failed/inoperable hard drives associated with IRS employees located in the Cincinnati, OH, area were sent to Martinsburg for destruction. Similarly, the hard drives associated with the Exchange 2003 Server decommissioned in May 2011, and associated backup tapes were sent to Martinsburg for destruction. Prior to May 2013, when the CTO changed the policy on destruction of media, Martinsburg degaussed media, and then collected it in a large, secure storage room until a significant volume had been accumulated. IRS Agency-Wide Shared Services then bid out contracts to outside vendors for the destruction of the media. According to the interviews of IRS managers [REDACTED] and [REDACTED], this occurred every year or year and a half prior to May 2013, when the policy was changed. Interviews of the IRS employees at Martinsburg and review of e-mails between employees revealed confusion relating to the CTO policy led to a staggered implementation of the degaussing of backup tapes and hard drives until June 2014, when both ceased at Martinsburg.

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 16

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

## REPORT OF INVESTIGATION

[REDACTED] the former Director of the IRS' DMSS Division, was interviewed regarding the handling and decisions to degauss tapes and stated that he was not aware of a specific policy in DMSS on excessing or destroying tapes they utilized. [REDACTED] stated DMSS followed the guidance provided in the Internal Revenue Manual (IRM) section 2.7.4, *Information Technology (IT) Operations, Magnetic Media Management*, with regard to the process for disposing of electronic media once it had been decommissioned or determined to be no longer useable.

The backup tapes containing "PII" were degaussed by IRS EOPS Media Management [REDACTED] personnel at Martinsburg, likely on, or shortly after, March 4, 2014, when the completed Form 3210 was received. At the time, the Media Management [REDACTED] was staffed by: [REDACTED] Lead Computer Assistant; and Computer Clerks [REDACTED] and [REDACTED]. [REDACTED] indicated that when these backup tapes were likely created, which was on or before May 2011, they were following the established policy, which was to preserve weekly backups for a six-month period. This means that these tapes likely contained full, weekly backups of the e-mail account for LERNER dating back to late November or December 2010. The practice of degaussing tapes at ECC-MTB continued until approximately June 2014, when a moratorium was put in place by local managers in an attempt to prevent accidental destruction of data in accordance with the CTO's May 2013 prohibitions relating to degaussing media containing e-mail information. The hard drives, however, were not degaussed because the IRS EOPS personnel had ceased degaussing hard drives in February 2014, as was their understanding of the CTO's May 2013 directive, which predated the receipt of the signed Form 3210.

Interviews and e-mail examinations revealed that [REDACTED] did not submit a timely Form 3210 with the shipment in January 29, 2014, because when the material was shipped from NCFB to Martinsburg, [REDACTED] was out of the office on leave for an extended period. When [REDACTED] returned to duty on or around February 17, 2014, he was asked by Martinsburg for the Form 3210, which he prepared and provided to Martinsburg in March 2014.

Interviews of, and e-mail traffic between, the IRS EOPS employees and other IRS employees indicated there was confusion about the status and requirements of the CTO's prohibitions. Interviews revealed that varying interpretations of the CTO's prohibitions led first to the cessation of degaussing all hard drives in February 2014 at Martinsburg, and subsequently the cessation of degaussing all backup tapes in June 2014. [REDACTED] staff, including the Media Management [REDACTED], consistently advised that the media was sent to them was for destruction, and because they would have no knowledge of what was contained on the media, the responsibility for preserving that information would have resided with the individuals who sent the media to them.

[REDACTED] was asked by TIGTA to attempt to find the degaussed tapes from the January 29, 2014, shipment. He stated that once items have been degaussed, they are placed in a storage area for eventual physical destruction. At the time of this request, he estimated that Martinsburg contained

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Treasury Inspector General for Tax Administration

Page 17

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



---

## REPORT OF INVESTIGATION

---

around 600,000 pieces of electronic media awaiting destruction, which included many thousands of tapes. Based on the physical description of what the old tapes looked like, IRS EOPS located the media in storage, and secured 424 tapes which were turned-over to TIGTA on February 20, 2015. On March 3, 2015, IRS EOPS personnel found an additional 49 tapes underneath brand new tapes, which were still stacked on the original pallets delivered on January 29, 2014.

In May 2011, the NCFB's Exchange 2003 Server's decommissioning process began and lasted approximately two years and ten months. Interviews indicated that although the Exchange 2003 Server was no longer operational, it remained powered on and functional as a backup, in case the new servers became unreliable. On October 11, 2011, [REDACTED], a Supervisory Management and Program Analyst, [REDACTED], e-mailed [REDACTED], an IRS IT Specialist, who was the representative from the IRS business unit responsible for the e-mail server, asking if the process for excessing the "Exchange SAN [Storage Area Network]" could begin; and, she responded in the affirmative. [REDACTED] IRS Server Share Support Unit, whose group was also responsible for equipment in the server room input an ITAMS ticket, which resulted in the server being powered off on November 1, 2011. [REDACTED] advised that he believed that all of the servers were removed from the NCFB's server room in late 2013.

Interviews of IRS employees involved in the search for the tapes and hard drives as well as those involved in the decommissioning process for the NCFB Exchange 2003 Server provided no evidence that the IRS employees involved intended to destroy data on the tapes or the hard drives in order to keep this information from Congress, the DOJ or TIGTA. No evidence was uncovered that any IRS employees had been directed to destroy or hide information from Congress, the DOJ, or TIGTA. However, the investigation revealed that the IRS did not put forth an effort to uncover additional, responsive e-mails. None of the IRS employees involved had been asked, prior to the June 30, 2014 request from TIGTA, to find any backup tapes, or the server hard drives associated with the NCFB Exchange 2003 Server, which would have contained responsive LERNER e-mails. The investigation determined that if the IRS would have conducted a search for the existence of backup tapes, they would have found the necessary backup tapes that contained LERNER's missing e-mails prior to when those backup tapes were degaussed in March 2014.

As a result of the technical challenges posed by the complexity of reassembling an unknown number of potentially damaged disk arrays, as well as the sheer volume of the data it represented, Kroll was contracted to recover any readable data from the 760 hard drives. As a result, approximately 12.5TB of data were recovered from the hard drives. After a review of the listings of recovered files, approximately 2.6TB of data in the form of MS Exchange database files were determined to be potentially relevant and subsequently further extracted for processing. From this additional data, five specific e-mail boxes belonging to IRS employees Nikole FLAX, [REDACTED], [REDACTED], [REDACTED], and [REDACTED] were recovered and filtered, resulting in 731 e-mail items sent to, copied to, or received from LERNER. A manual comparison to de-duplicate these items against

---

Case Title:  
EXEMPT ORGANIZATIONS DATA LOSS

Case Number:  
54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 18

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

the IRS production to Congress resulted in the discovery of 58 new e-mails that had not been previously provided to the Congress, the DOJ or to TIGTA.

The 424 tapes from the NCFB MS Exchange Server and the 49 other miscellaneous tapes that were discovered on the same shipment pallet were provided to Kroll for analysis; two tapes out of the 424 had recoverable data. One appeared as though it was damaged or may have been encrypted. According to IRS EOPS, the capability to encrypt Exchange backup tapes was not available during the time this tape would have been in use. This would indicate the tape would have belonged to another IRS group. Since the identifying labels were removed prior to degaussing, TIGTA was unable to determine the actual source or business unit owner of the tape or the possible location of its encryption keys. The other readable tape contained e-mail backup files created in January 2011, but were for IRS employees outside of the scope of this investigation. The 49 miscellaneous tapes were also analyzed and contained data from no later than 2003, which is also outside the scope of this investigation.

### ***BlackBerrys***

TIGTA took possession of LERNER's BlackBerry on June 10, 2013, after she left the IRS. This BlackBerry was assigned to LERNER on February 17, 2012. Forensic examination of the BlackBerry provided 2,972 readable e-mails. A manual comparison to de-duplicate these items against the IRS production to Congress resulted in the discovery of 190 new e-mails that had not been previously provided to the Congress, the DOJ or to TIGTA; 169 of the e-mails are from after 8:30 AM on May 16, 2013; six of the e-mails mentioned EO matters, but nothing responsive to Congress' request. TIGTA identified the BlackBerrys assigned to LERNER prior to the one TIGTA obtained on June 10, 2013. The investigation determined that the prior BlackBerrys issued to LERNER were more than likely destroyed when LERNER was issued a new one on February 17, 2012.

Interviews were conducted to determine if any e-mails could possibly reside on the BlackBerry server. The investigation determined that the BlackBerry server did not retain copies of e-mail traffic; rather it served as a router and conduit for e-mails getting to and from the device only. No e-mails were recoverable from this source.

### ***Loaner Laptops***

Interviews indicated a possibility LERNER had been assigned a "loaner" laptop while her laptop was being serviced. Nine computers, which were used by the IRS as loaner systems for employees who had suffered significant malfunctions were seized and forensically analyzed. A tenth loaner laptop had since been refurbished, and in doing so, the hard drive had been sanitized according to IRS policy and therefore forensic examination was not beneficial. Forensic analysis of the nine laptops found no indication LERNER herself had ever used them, although 137 e-mail items from other

---

Case Title:  
**EXEMPT ORGANIZATIONS DATA LOSS**

---

Case Number:  
**54-1406-0008-I**

TIGTA Form OI 2028R (Rev. 04/2007)

Page 19

Treasury Inspector General for Tax Administration

### **OFFICIAL USE ONLY**

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

temporary users relating to e-mail communications and meeting notices involving LERNER were recovered and reviewed. A manual comparison to de-duplicate these items against the IRS production to Congress resulted in the discovery of 75 new e-mails that had not been previously provided to the Congress, the DOJ or to TIGTA.

### ***Offsite Contractor Storage of Backup Tapes***

During the course of this investigation, interviews also revealed the IRS utilized contractor Iron Mountain for offsite storage of backup media possibly from the late 1990s through 2012 or 2013, under numerous contracts for different locations and different business units. During some of this period, Iron Mountain was used to store backup tapes from the NCFB MS Exchange Server. Although [REDACTED] thought it was a possibility that some backup tapes pertinent to the investigation were maintained by Iron Mountain, the investigation determined this was not the case.

### ***Network Transaction Logs***

TIGTA was also able to identify the existence of e-mail header transaction logs in the possession of both the GSOC and Treasury contractor, AT&T. These logs were routinely collected by network operations personnel for the purpose of conducting network security monitoring activities, such as the detection of malicious e-mail activity. These transactional logs included the From, To, Date/Time and Subject line fields of all e-mail messages that come in and out of the IRS enterprise network. No message body, content or e-mail attachments were collected by the logs. After a technical comparison of these logs against the IRS production to Congress and of the e-mails obtained by TIGTA from the backup tapes, exchange server hard drives, LERNER's BlackBerry and the IRS loaner laptops, TIGTA estimates that the location of between 23,000 and 24,000 e-mails sent or received by LERNER could still be missing. Of those e-mails still not recovered, 4,274 were from 2010; 11,560 were from 2011; 7,952 were from 2012; one was from 2013.

### **Federal Records Management Act Compliance**

#### ***Microsoft Office Communications Server***

As an additional area of investigative interest, the online communications or OCS "chat" software utilized by IRS was investigated to identify any data that could be recovered from online communications associated with LERNER or other IRS employees. In addition, the investigation reviewed if the IRS had a duty to record and preserve as records OCS chat dialogue between IRS employees. IRS IT and the IRS Office of Chief Counsel confirmed LERNER, like most employees, had access to OCS, but stated OCS conversations and the usage history are not recorded by the IRS.

---

Case Title:  
**EXEMPT ORGANIZATIONS DATA LOSS**

---

Case Number:  
**54-1406-0008-I**

TIGTA Form OI 2028R (Rev. 04/2007)

Page 20

Treasury Inspector General for Tax Administration

### **OFFICIAL USE ONLY**

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.



---

## REPORT OF INVESTIGATION

---

An MOU between the IRS and the National Treasury Employees Union regarding the implementation of OCS, was executed on July 30, 2010, and went into effect later in 2010. OCS was an office collaboration software suite that integrated with existing MS Office products already in use within the IRS, such as MS Outlook for e-mail and MS Office for document creation and editing. Included within the features provided by OCS were an instant messaging function and the ability to engage in "live" online meetings and document sharing and collaboration. The terms of the MOU dictated that the IRS would not log or record the contents of OCS instant messages, would not record any online meetings without prior warning to all participants, and would not use OCS to track employee availability or productivity.

The investigation revealed the OCS sessions were not written to a server and the only way information from an OCS session between employees would be recoverable is if one of the participants cut and pasted the session into an e-mail or other document or if it was written to one of the employee's hard drives. The investigation was unable to recover any of the OCS sessions that may have occurred between LERNER and other employees.

### *Policy Regarding Records and Records Retention*

[REDACTED], former Supervisory Management and Program Analyst, IRS, Records and Information Management, stated the National Archives and Records Administration (NARA) considers e-mail as a "format or mechanism to automate messaging information," and therefore does not consider e-mail as a series of records unless it has been categorized as a record. [REDACTED] explained NARA guidance regarding e-mail retention is based on applications outlined in Department of Defense (DoD) directive 5015.2. The directive indicates agencies should categorize e-mails into "subject files" and link these files to a traditional record series found in the Record Control Schedules (RCS). NARA considers e-mail as a "format or mechanism to automate messaging information," and therefore, does not consider e-mail as a series of records unless placed into such "subject files." When agencies cannot meet the parameters outlined in DoD 5015.2, NARA recommends that end-users "print and file" long-term records, to include the metadata contained in the e-mail, and dispose of them in compliance with their agency's RCSs. NARA also recommends that end-users "drag and drop" e-mails they wish to retain and then dispose of them when no longer needed for current business.

Paul WESTER, Chief Records Officer, NARA, was interviewed and he opined the IRS did nothing wrong as far as safeguarding records. WESTER stated the only thing the IRS did not do was to report the loss of data to NARA, but there is no timeframe for agencies to report the loss. NARA wants agencies to employ due diligence to recover and/or identify the records before filing a report. WESTER also stated NARA does not want agencies to report every hard drive failure, especially without first trying to determine what was lost. When told that between 2009 and 2011, the IRS did not have the technology to implement a DoD 5015.2 Standard compliant e-mail system and that the

---

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 21

Treasury Inspector General for Tax Administration

OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.

---

## REPORT OF INVESTIGATION

---

direction to "print and file or click and file" was the prescribed method of records retention, WESTER stated this falls within NARA's guidance.

The fact that the IRS utilizes OCS for instant messaging and does not log or record it, is not necessarily a violation of NARA's guidance. NARA does not issue specific guidance or policy to dictate what or how much should be saved electronically. NARA provides guidance as it relates to records management, which applies to OCS. Whether OCS is being used according to NARA's guidance, depends on how OCS end-users are utilizing the program. It is difficult to say definitively if the IRS is violating NARA's guidance by not logging or recording OCS, but it is necessary for the IRS to manage OCS to meet Federal Records Management Act requirements.

Case Title:

EXEMPT ORGANIZATIONS DATA LOSS

Case Number:

54-1406-0008-I

TIGTA Form OI 2028R (Rev. 04/2007)

Page 22

Treasury Inspector General for Tax Administration

### OFFICIAL USE ONLY

THIS DOCUMENT IS PROVIDED FOR OFFICIAL USE ONLY. ANY REQUEST FOR DISCLOSURE OR FURTHER DISSEMINATION OF THIS DOCUMENT OR INFORMATION CONTAINED HEREIN SHOULD BE REFERRED TO HEADQUARTERS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION.