

**FEDERAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL**



AUDIT REPORT

**REVIEW OF FTC POLICIES AND PRACTICES
TO REMOVE SENSITIVE INFORMATION
FROM SURPLUSED HARD DRIVES**



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

Office of Inspector General

January 31, 2001

Chairman Pitofsky;

The Office of Inspector General (OIG) has completed a review of the Federal Trade Commission's controls over the release of information stored on the hard drives of "excessed" or "surplused" computers. Computers deemed to be outdated by the FTC are usually made available to school districts free of charge for word processing and internet access. The objectives of this review were to:

- Determine whether hard drives in surplus computers that have been relocated to FTC's warehouse contain non-public and/or sensitive information;
- Determine whether procedures in place to scrub hard drives are complete and universally performed on all computer hard drives; and
- Identify the level of sophistication required to obtain information from any hard drives that are found not to have been scrubbed.

The OIG was assisted on this technical review by the Urbach Kahn & Werlin, LLP's Systems Audit and Consulting Group (SACteam). The SACteam found that the procedures followed by agency staff to scrub the hard drives before releasing them need improvement. For example, in a sample of 26 hard drives, five contained easily accessible files and internal systems data, including password and configuration files and case specific documents such as subpoenas. All five were ready for release outside the agency. In addition, the audit team found another five hard drives that, due to ineffective erasure techniques used through 1999, contained files that could still be downloaded. This finding suggests that hundreds of computers that have already been released to Washington D.C. schools in August of 1999 could contain nonpublic information.

In keeping with OIG direction, the methods of data recovery utilized by the SACteam require only basic computer hardware familiarity, tools and skills, but no "high-end" technologies or advanced training.

Aside from the risk of releasing non-public information through a donation program, there are also real dollar costs associated with preparing computers for release outside the agency. In addition to the technician's time to ensure the computer works and to scrub the hard drive, there are also costs to store and ship the computers. Further, schools often lack the personnel to set up the computers and are often required to wait months for needed assistance from school system technicians. An alternative is to seek assistance from FTC technicians - yet another cost.

Concern over the appropriateness of the program has increased recently because of revelations in the newspapers regarding missing computers donated by Federal agencies to Washington D.C. schools. The D.C. inspector general's office found during a two month study of 12 schools that neither principals nor the school warehouse could find 88 percent of the computer equipment the U.S. government had donated to those schools in the past two years.

Given the expense and vulnerability of this program, the OIG believes that the agency would be better served by scrapping outdated computers and destroying all hard drives.


On the other hand, if management believes that moving away from this voluntary program is not the solution, then, at a minimum, OITM should implement the recommendations developed by the SACteam to address the vulnerabilities identified. These steps include formalizing policies and procedures to ensure uniformity and completeness of the data erasure and retesting all "purged" hard drives for data accessibility.

We conducted our fieldwork in September/October, 2000. The review was performed in accordance with Government Auditing Standards issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to provide an independent and systematic assessment of the performance of the activity being reviewed, and to obtain reasonable assurance that the organization's internal control structure over safeguarding assets is suitably designed and implemented to achieve the control objectives.

Our findings and recommendations were discussed with program managers during the review to minimize the agency's vulnerability to the unintentional release of sensitive or privacy information. Management's comments to these findings and recommendations are attached to the audit report. These comments include technical corrections, which we have incorporated in the report, and issues raised by ITM managers regarding our sample selection, the agency's responsibilities to implement the *Computers for Learning Program*, and the costs and risks associated with the program. The OIG has addressed these issues in a separate document appended to this report.

The OIG appreciates the assistance provided by OITM managers and staff, and to staff at the FTC warehouse in Alexandria, VA, throughout our review.

Respectfully submitted,


Frederick J. Zirkel
Inspector General



**FEDERAL TRADE
COMMISSION**

**Federal Trade Commission
Office of Inspector General**

**Review of FTC Policies and Practices
to Remove Sensitive Information from
Surplused Hard Drives**

UK
&W Urbach Kahn & Werlin LLP
CERTIFIED PUBLIC ACCOUNTANTS

SACTEAM

REVIEW OF FTC POLICIES AND PRACTICES TO REMOVE SENSITIVE INFORMATION FROM SURPLUSED HARD DRIVES

Urbach Kahn and Werlin, LLP's Systems Audit and Consulting Group (the UKW SACteam) was contracted by the Federal Trade Commission Office of Inspector General (FTC/OIG) to perform a review of FTC policies and practices to remove sensitive information from surplused hard drives. The objectives of the review were to:

- Determine whether hard drives in surplused computers that have been relocated to FTC's warehouse contain non-public and/or sensitive information,
- Determine whether procedures in place to scrub hard drives are complete and universally performed on all computer hard drives, and
- Identify the level of sophistication required to obtain this information from the hard drives.

The Federal Trade Commission's scope of responsibilities as a Federal agency includes enforcing a variety of federal antitrust and consumer protection laws. The agency's work is legal in nature and is subject to not only confidentiality laws but also to privacy laws (i.e. Privacy Act information). Therefore, the need for protecting sensitive data both in hardcopy and electronic form is critical.

Compromising non-public/sensitive data could occur in numerous ways, not just by 'hackers gaining information electronically by reaching FTC systems from the Internet. Many government agencies and private corporations surplus their outdated computers for donation to schools and/or nonprofits¹, or sell them as scrap. Unless specific precautions are taken, the data contained on those hard drives might remain intact, and possibly accessible to the receivers of the surplus equipment. There may still be readable files on the disks containing sensitive financial or legal data, data protected from disclosure under Federal law, or information about the internal structure of the originating organization's internal network, including employee and system passwords. Unfortunately, as recent disclosures in the mass media illustrate, it usually takes an embarrassing security breach before a company begins to adopt better network and hardware security practices. The SACteam's review of FTC's surplus hard disk clearing process indicates that while there are procedures in place, they require improvement.

¹ Executive Order 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*, streamlines the transfer of excess and surplus Federal computer equipment to schools. One such avenue, the "Computers for Learning" website, allows schools and educational nonprofits to register to request surplus Federal computer equipment. Federal agencies can then use the website to donate computers to schools and educational nonprofits based upon indications of need. The web site for the program is <http://computers.fed.gov>.

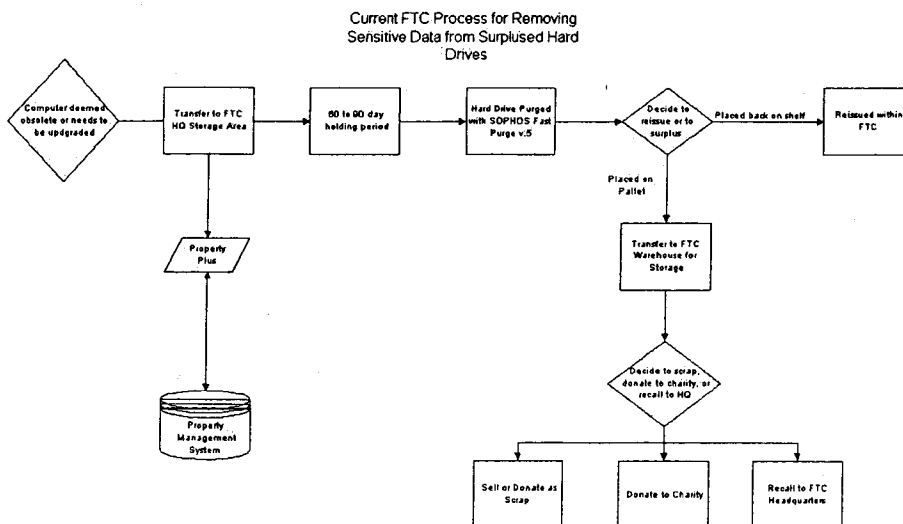
FTC Policies and Practices

Currently the Office of Information and Technology Management's (OITM) Litigation and Customer Support Branch receives computers from within the FTC when they are deemed obsolete, are damaged or need to be upgraded. Computer systems and individual hard drives are transferred, agency-wide, to a secured storage area at the FTC headquarters at 600 Pennsylvania Avenue. Property management software, called "Property Plus," is used to maintain an inventory of received and shipped computers. Once in the storage area, computers are generally held for approximately 60 to 90 days before a formal purging process begins. The holding period allows the former owners of the computers a window of time to ensure no valuable files were left on the equipment being replaced.

After the holding period ends, based on a process implemented within the last few months, the hard drives are "wiped" using a commercial software product called SOPHOS -- Fast Purge v.5. The software works by overwriting the data area on the hard disk with random characters, thereby making recovery of readable information difficult or impossible by conventional methods. Five such wipes must be performed to comply with government standards, as identified in the SOPHOS product manual and FTC policy.

Once SOPHOS has wiped the hard drive, the computer is marked as "Degaussed" or "Purged" by the staff and either placed back on the shelf for reissue within the FTC, or loaded onto a pallet for transfer to the FTC Warehouse in Alexandria, VA. Once at the warehouse, the computers are stored until they are (1) sold as scrap, (2) given to nonprofit/educational institutions, or (3) reissued within the FTC.

The flowchart below represents current FTC practices for the sanitation of hard drives. As noted, it has only been in place for a few months. Prior to this time frame, hard drives were cleared by means of the FDISK and FORMAT commands at the command prompt. FDISK and FORMAT are system utilities shipped with the Microsoft Windows operating system. FDISK can be used to erase the existing data partitions on the hard drive and FORMAT can be used to remove files by re-initializing the new data partition to appear unused. It was recognized that FDISK/FORMAT alone would not be sufficient to make files unrecoverable, so the SOPHOS product and procedures were acquired and deployed.



Whether the computer would be donated or reissued, an operating system, such as Windows 3.x (for donated computers) and Windows NT (for hard drives slated for reuse within the agency), would be installed on the cleared hard disk. Computers to be reissued are labeled "SID" (Security Identification Number) to indicate they are ready to be set up for network access. The "SID" is used by Microsoft to control the licensing of its software products. At the FTC, the SID also uniquely identifies the user, group, service and computer accounts.

Our review was intended to determine whether there were weaknesses in either the current or previous clearing procedures that might result in recoverable data being found on machines after they should have been properly cleared for disposal beyond FTC's control (i.e., to salvagers or charitable organizations). Machines reissued internally would not present similar disclosure concerns.

Sampling/Testing Methodology

The SACteam extracted a sample of 26 hard drives, of approximately 150 total hard drives, from various locations within the FTC warehouse in Alexandria, VA. Of the 26 sampled hard drives, five were "loose" and the remaining 21 were located in existing PCs.²

Hard drives located in computers were "cold-booted" to establish if the computer was in working condition, and we noted that none of those sampled would boot without a system disk.³ Not being able to boot from a system disk does not necessarily mean that data cannot be recovered, and may provide a false sense of security since a user might assume that no further clearing is needed. The pulled hard drives were placed into paper bags and labeled with FTC number, serial number, time, date and location then transferred to the SACteam's offices in Washington, D.C. for further testing.

The SACteam performed the following for each hard drive:

- *Set the sampled hard drive to "slave" and attached it to a test machine.*

Setting a hard drive to "slave" enables it to be attached to an existing computer and viewed as a second hard drive. The process involves moving circuit "jumpers" to specific settings on the hard drive. Essentially, this is the equivalent of adding a second hard drive to a computer, and allows the drive to be read non-invasively (i.e., essentially in read-only mode).

- *Used Easy Recovery by Ontrack and other utilities to establish the "recoverability" of files.*

² See Attachment A for more detailed testing information. Attachment B contains a list of select files available on surplus computers tested by the OIG.

³ A system disk is used to boot a computer with a damaged or nonexistent operating system and generally contains utility programs that can help recover damaged or lost files on the system. "Bootable" system disks can be created from any computer running Microsoft Windows.

Easy Recovery is a powerful software utility used to recover deleted/purged files from hard drives that have been FDISKed, reformatted, etc. The software is available for download from <http://www.ontrack.com> and is offered in a trial version that allows the recovery of up to five files for free. Norton Utilities was also used in some cases. The Easy Recovery software is not compatible with Small Computer System Interface (SCSI) drives, but Norton Utilities can be used instead. Most of the drives sampled were Integrated Disk Electronics (IDE) drives.

At no time was any data modified, moved, or altered in any manner on the sampled software. The recovery software runs entirely on the host machine to preserve the original state of the hard drive.

- *Created a report of all files recovered from each hard drive.*

The Easy Recovery software creates a report of all files that were recoverable and potentially readable. The reports detail the file name, original creation date, size and location. In cases where Easy Recovery was not used, i.e. with SCSI drives, the directory listings were dumped to a text file by using the simple DOS command `dir d:\ > list.txt`.

The methods of data recovery performed by the SACteam would require basic computer hardware familiarity, tools and skills, but no "high-end" technologies, advanced training or certifications. The hardware configuration used during testing, i.e. setting the sample drives as "slave," requires knowledge of circuit jumpers and settings which the average person may not possess; however, supporting information for specific drives and drive controllers is generally freely available on the Internet.

If the sample hard drives were already installed in a computer with a working operating system, the level of knowledge needed to find recoverable files would decrease significantly. The latter case would simply involve installing recovery software and running the program.

Findings and Recommendations

The SACteam noted the following during our review of FTC policies and practices for removing sensitive information from surplus hard drives.

1. Five hard drives marked as "Degaussed" contained recoverable data.

Five of the 26 sampled hard drives marked "Degaussed" contained recoverable data (e.g. all files could be downloaded and viewed/printed). We found numerous system and document files on these hard drives. File names such as "subpoena.ltr," "network.cfg," "legal.ltr," and ".pwl" were found on drives marked as "Degaussed." (See Attachment B.)

This discovery is quite significant because these hard drives were deemed ready for donation or sale as scrap, but were clearly not processed according to the procedures described as FTC policy. Specifically, the pwl files (password list), configuration files, and legal document file names should be a source of concern. Passwords can be recovered from a pwl file through the use

of freely available "password cracking" utilities. Additionally, the configuration and document files may contain network configuration settings, modem/RAS numbers, Privacy Act information, internal IP address schemes and other potentially sensitive data. Releasing this information outside of the agency could provide an interested party with a potential roadmap into the FTC's internal network.

OMB Circular A-130, Appendix III requires Federal Agencies to adequately protect their information systems. The level of protection drops significantly when sensitive configuration files could potentially be accessed by anyone after entering the public domain.

2. Five hard drives marked as "C", "SID", or unmarked contained recoverable data.

Five of the 26 sampled hard drives marked as "C", "SID", or unmarked contained recoverable data. These machines had not been wiped with the SOPHOS software. FTC Technical Operations staff had indicated that the process of wiping all machines at the warehouse using SOPHOS was ongoing. Numerous system and document files were discovered on these hard drives.

3. Current FTC practices for removing sensitive data from hard drives lack formal documentation and control structure.

The Office of Information Technology Management lacks formalized documents describing the internal procedures for clearing sensitive data from surplus computers. The process we described above is said to exist, but it has not been formalized or approved by management. The current process appears to be an improvement over the previous process. However, the process needs to be formally documented and more controls need to be established to ensure that each hard drive is purged appropriately.

Organizations should have procedures in place to remove sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. If this non-public/sensitive data is not removed, it may be recovered and inappropriately used or disclosed by individuals who have access to the discarded or transferred equipment and media.

4. Additional hard drives marked as "Degaussed" may contain sensitive data.

Computers transferred to the warehouse prior to the implementation of SOPHOS were simply reformatted and perhaps re-loaded with Windows 3.x. The SACteam was informed that the Technology Operations team was in the process of using the SOPHOS purge software to clean the hard drives that were transferred to the warehouse prior to the implementation of the new practices. Contracted employees had been assigned to perform this task. A "mass" operation of wiping all hard drives at the warehouse with SOPHOS occurred in the Summer of 2000. However, the process was not documented, and it appears that some of the drives were marked as "degaussed" without being appropriately purged. As a result, we must assume that drives in machines that were shipped to salvagers or charities prior to the institution of the new clearing

process could have contained sensitive information. We were advised that the last such shipment was during the winter of 1999-2000.

Recommendations

We recommend FTC management:

1. Systematically re-examine the hard drive population to ensure that all data has been appropriately purged by the SOPHOS software. This is a necessary and critical step that should be completed prior to any computers being released from the warehouse. Alternatively, based on cost and resource considerations, it may be more practical to destroy the hard drives. If viable machines are to be donated, the cost of providing and installing replacement drives may be lower, and will present less risk, than relying on the clearing process.
2. Develop formal policies and procedures for the removal of sensitive information from hard drives and establish a stronger control structure. The flow chart presented above represents the basic procedure flow, but a more detailed policy needs to be developed and approved that covers procedures in detail. Also, standard forms or a log should be used to document that all discarded or transferred items are examined for sensitive information and that this information is cleared before items are released. For example, checklists specific to each computer requiring a signature stating that the data has been appropriately deleted could be implemented. This would increase controls by clearly assigning responsibility for a specific computer to a specific individual. Again, simply destroying the drives should be considered an option, although the logging procedure confirming disposal should in any event still be followed.
3. Establish procedures for periodically examining computers at the warehouse to ensure all data has been appropriately wiped. These examinations should be unannounced and random in nature. This would add an additional layer of assurance to the hard drive sanitation process at the FTC.
4. Management should consider whether there may be a benefit to following up with any of the outside recipients of surplus FTC computers over the last year to confirm whether the drives actually do contain recoverable sensitive data. Such an investigation would need to be highly confidential in nature. We note the recent disclosure that one of the recipients of Federal surplus computers, the Washington D.C. school district, was found to be unable to determine the whereabouts of the equipment⁴. Clearly, this further complicates the potential reach of accidental disclosure if the FTC's computers were among those "lost."

⁴ Attachment C displays an article entitled "D.C. Schools Mislplace Donated Computers," *Washington Post*, October 13,2000.

FTC Warehouse Information

Sample #	Date	FTC Tag Number	Serial Number	Bootable	Marking	Comments	Location	Data recovered?
1	9/22/00	B009989	CCC 0402899	No	Unmarked	No Video	Top Shelf B-1	Yes
2	9/22/00	10000326041	CCC 0402931	No	Unmarked		Top Shelf B-1	No
3	9/22/00	10000341364	UTI9705079	No	Degaussed		A	No
4	9/22/00	B00194	N/A	No	Degaussed	No Video	B5	No
5	9/21/00	N/A	L409W0SS	No	Unmarked			No
6	9/21/00	10000306919	CCC0402897	No	Degaussed 7/20			No
7	9/22/00	N/A	9535100097	N/A	Degaussed	HD from DG Box	B-bottom location	Yes
8	9/22/00	N/A	9533100215	N/A	Degaussed	HD from DG Box	A	Yes
9	9/22/00	N/A	2110S P/N TM21S011	N/A	Unmarked	HD from Box found at B3	A	Yes
10	9/22/00	N/A	9533100196	N/A	Unmarked	HD from Box found at B3	B3	Yes
11	9/22/00	N/A	9537100140	N/A	Unmarked	HD from Box found at B3	B3	Yes
12	9/21/00	10000299810	114418	No	Degaussed	HD from DG Box	A	Yes
13	9/21/00	B00435	4X0-10446	No	SID	Disk boot failure	A	Yes
14	21-Sep	B009179	4X0-11708	No	Degaussed	Drive not ready error	B4	No
15	21-Sep	10000334933	114477	No	Degaussed	Drive not ready error	B4	Yes
16	21-Sep	10000312788	CCC0401999	No	Degaussed	Disk boot failure	A	No
17	9/21/00	10000300130	114377	No	Degaussed	Disk boot failure	B4	No
18	9/22/00	10000335059	CCC0401797	No	Degaussed	Disk boot failure	A	No
19	9/21/00	10000318504	CCC0402894	No	C		A	No
20	9/21/00	10000302780	CCC0401860	No	Clean	Disk boot failure	B1	Yes
21	10/6/00	10000318274	CCC 0401996	No	Purged	Disk boot failure	B5	No
22	10/6/00	10000336753	CCC 0402978	N/A	Degaussed 7/20	Disk boot failure	B4	No
23	10/6/00	B005268	CCC 0402958	N/A	Degaussed 7/19		Pallet B4 Bottom	No
24	10/6/00	N/A	CCC4102638	N/A	Degaussed 7/21		Pallet B4 Bottom	No
25	10/6/00	10000306045	CCC0402919	N/A	Degaussed 7/20		Pallet B4 Bottom	No
26	10/6/00	B009104	CCC0402951	N/A	Degaussed 7/21		Pallet B5 Bottom	No
				N/A	Degaussed 7/20		Pallet B5 Bottom	No

Sample of Recoverable Files
from Four FTC Hard Drives

FILE NAME	SAMPLE #	FILE SIZE	FILE DATE
EYESONLY.WPG	1	8 KB	03\25\96
ACCESS.LTR	1	608 Bytes	12\22\95
PROTOCOL.INI	1	1 KB	06\27\94
NETWORK.INF	1	36 KB	10\01\92
PLEADING.WPT	1	56 KB	03\25\96
RESUME1.WPT	1	9 KB	03\25\96
RESUME2.WPT	1	9 KB	03\25\96
CONGRES1.WPT	1	112 KB	01\18\96
CONGRESS.GRP	1	16 Bytes	01\18\96
FTC.GRP	1	6 Bytes	01\18\96
FTC.WPT	1	51 KB	06\05\96
FTCSEAL.WPG**	1	17 KB	01\18\96
CLASSIFI.WPG	1	7 KB	03\25\96
CONFIDEN.WPG	1	3 KB	03\25\96
CREST.WPG	1	2 KB	03\25\96
LEGAL.LTR	10	39 KB	04\19\96
HOSTS	12	737 Bytes	08\02\96
NETWORKS	12	407 Bytes	08\02\96
PROTOCOL	12	800 Bytes	08\02\96
SERVICES	12	5 KB	08\02\96
LMHOSTS.SAM	12	3 KB	08\02\96
SWITCH.INF	12	6 KB	08\02\96
RASREAD.TXT	12	51 KB	08\02\96
RAS.ICO	12	766 Bytes	08\02\96
MODEM.INF	12	248 KB	08\02\96
WEBBING.RPT	14	3 KB	09\20\95
ANNE.RPT	14	9 KB	10\05\95
SUBPOENA.LTR	14	2 KB	09\29\95
ALMACS.RPT	14	2 KB	09\19\95
FLEET.RPT	14	3 KB	09\20\95
HEARING.QUE	14	8 KB	09\22\95
GTECH.RPT	14	6 KB	09\29\95
HILLARY.1	14	5 KB	11\08\95
LMUSER.INI	14	64 Bytes	06\27\94
LANMAN.INI	14	967 Bytes	06\27\94
BMCDONOU.PWL*	14	606 Bytes	06\27\94
DML.PWL	14	606 Bytes	06\27\94
WMCDONOU.PWL	14	606 Bytes	06\28\94
MDC.PWL	14	606 Bytes	06\30\94
BMCCARTH.PWL	14	606 Bytes	09\01\94
ACAVERLY.PWL	14	606 Bytes	08\31\94
DBARRY.PWL	14	626 Bytes	01\22\96
PWOOD.PWL	14	606 Bytes	01\14\95
PWOOD000.PWL	14	606 Bytes	04\19\95
PBLOCK.PWL	14	606 Bytes	04\19\95
JARLEO.PWL	14	606 Bytes	04\20\95

** The WPG file extension denotes a graphic file. These files could represent letterheads and other official seals.

* PWL files (Password List) contain weakly encrypted Microsoft Windows passwords that can be recovered using free software downloadable from the Internet.

D.C. Schools Misplace Donated Computers

By Carol D. Leonnig and Justin Blum
Washington Post Staff Writers
Friday, October 13, 2000; Page B01

District public schools cannot locate nearly 260 pieces of computer equipment that the federal government and two major grocery store chains donated to help students meet the challenges of a high-tech era, according to an audit released yesterday.

The D.C. inspector general's office found during a two-month study of 12 schools that neither principals nor the school warehouse could find 88 percent of the computer equipment the U.S. government had donated to those schools in the past two years. Five schools were missing equipment, including 62 computers that cannot be found at Spingarn STAY Senior High School, a night school program in Northeast, and 48 computers slated for Shadd Elementary School in Southeast.

The auditors also focused on computers donated by Giant and Safeway charity programs to six other schools in the last two years, but they found far fewer problems. The inspector general tried to track 84 pieces of store-donated equipment, worth \$880,000; auditors found five computers missing from two schools, Barnard Elementary in Northwest and Anacostia Senior High School in Southeast.

In one instance, auditors found that 83 computers donated by a federal agency for Anacostia High were instead given to a church member and a person who said she was a school employee. The inspector general's office declined to identify the two individuals but indicated that the matter was serious.

"While I will not confirm or deny that there is an ongoing investigation, I would say the IG has the discretion to open an investigation based on audit findings which show there is a suspicion of fraud or misconduct," said Gloria Johnson, a spokeswoman for the inspector general's office.

Overall, the audit found that school officials "were not adequately controlling donated property," Inspector General Charles C. Maddox wrote to School Superintendent Paul L. Vance. "School officials . . . could not fully account for the federal property received, did not maintain inventory records" and did not properly report disposing of the equipment.

Vance said he did not know what happened to the computers, which vanished before he took over, and said the school system needs to put in place policies that will allow it to account for equipment.

"It's not rocket science," Vance said. "It's Management 101. We certainly have the technological capacity of doing it. I can assure you we're going to do it."

In a letter to Maddox, Vance promised a number of policy changes. He said he would instruct the director of logistical support services to reconcile the equipment disparities with the central inventory record, conduct periodic checks of inventory and ensure bar-coding of school property.

Among the examples cited in the audit was a donation by the U.S. Treasury Department of 62 pieces of excess equipment, mostly Pentium 133 computers, to Spingarn STAY Senior High

School in February. Auditors visiting in May found that the employee responsible for the equipment didn't know where it was.

"This individual contends that warehouse center personnel mistakenly took the Treasury computers as part of the shipment scheduled for disposal," the audit says.

A spokesman for Rep. Thomas M. Davis III (R-Va.), chairman of the House Government Reform subcommittee on the District, said the congressman is troubled by the report but confident that Vance will resolve the matter.

The audit suggests that the \$880,000 in supplies and equipment donated by Giant and Safeway in the past two years did make it to designated schools, as shoppers had intended when they saved store receipts and earmarked specific schools to benefit. But a Giant official said she was "obviously concerned" about the lack of an inventory and the missing computers. Giant has donated more than \$500 million in computer equipment to schools in the region since it began an "Apples for the Students" program in 1989.

"It was equipment that was basically earned by the shoppers, the parents of the children," Melanie Gness said. "If the equipment's not available for their children, and their grandchildren, then the program's not working as it was intended to work."



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

December 18, 2000

Memorandum

To: Fred Zirkel, Inspector General
Office of the Inspector General

From: Richard Turner
Chief Information Officer

Subject: Comments on Draft Audit Report Review of FTC Policies and Practices to
Remove Sensitive Information from Surplused Hard Drives

This memorandum provides comments on the draft audit AR01-049. The comments reflect an interpretation and clarification of the findings. These comments however are not intended to bring into question the conclusions of the audit. We agree that a thorough review of practices with the implementation of new policies to ensure proper handling of potentially sensitive information is necessary and is a priority of this office.

Background

In the past, ITM has scrapped PCs through GSA programs rather than directly donate the excess to any non-federal public institution. In August of 1999, the FTC released systems to three public institutions: Shaw Junior High School, Sousa Middle School and Turner Elementary School. Those systems were Intel based 486 - 66 units re-formatted with a Microsoft Windows for Workgroups operating system version 3.11. The systems were moved to the FTC Alexandria warehouse as excess equipment subsequent to the comprehensive upgrade of desktops to Microsoft Windows NT 4.0. That effort started in November of 1997 and was complete by June of 1998.

As noted in the report Executive Order 12999 streamlines the transfer of excess and surplus Federal computer equipment to schools. But it is also worth noting that GSA is encouraging use of the program through periodic mailings or advertisements to agencies highlighting the advantages of the program to the agency and recipients. In addition, the Federal Management Regulation 102-36, Disposition of Excess Personal Property, 102-36.295 requires the annual submission of the Non Federal Recipients Report and 102-36.475 requires the Chairman to report all Computers for Learning transfers to GSA. The assumption being that it is the

policy of the Executive branch to encourage this activity and GSA tracks the contributions. The following are specific comments and recommend changes organized by the heading in the report.

Cover Letter to Chairman Pitofsky

The letter indicates that "schools lack the technical skill to connect the computers to the Internet." It has been our experience that schools in this area do have surprising knowledgeable staff and volunteers with extensive experience in interfacing equipment to the Internet. Fairfax County, for example, assigns technical staff to support individual schools. Although it is true that schools do not have enough staff to test and configure all equipment, they appear to set priorities and focus strictly on the best donations. The letter further indicates that schools ask for assistance from the FTC. ITM does not provide technical assistance to the schools that have received excessed equipment, but have answered basic questions about the configuration and quality of that equipment. Any "additional cost" to respond to those questions would be less than minimal.

FTC Policies and Practices

Page 2, *change* "Currently the FTC's Technology Operations team" to "Currently the FTC's Litigation and Customer Support Branch."

Page 3, clarification on the statement "the computer would be reissued or donated, and operating system, such as Windows 3.x would be installed on the cleared hard disk." Hard drives slated for reuse would be re-imaged with Windows NT. The Windows 3x operating system is loaded only on systems designated for donation.

Page 3, correct statement " the SID of a machine must be reconfigured to match the software license." The SID has nothing to do with the control of licensing. The SID uniquely identifies user, group, service and computer accounts within an enterprise.

Sampling and Testing

From the audit the SAC team extracted a sample of 26 hard drives of approximately 150 total hard drives, from various locations in the FTC Alexandria warehouse. The draft report implies that ITM believes that all of the systems and drives stored in the warehouse had been completely purged of data and were ready for disbursal. However, during interviews, ITM staff informed the SAC team that systems and drives at the warehouse certainly may contain accessible data since the purging effort was a work in progress.

As a further clarification, ITM staff treat the FTC warehouse as a secure storage area similar to the way staff treat the Room B-3 repair area in the Headquarters building. Although there are no guards at the warehouse, access is restricted and FTC staff are on site during business hours, otherwise the facility is locked.

Clarification is necessary on page 4 under heading "Created a report of all files recovered from each hard drive." The report states the "software creates a report of all files that were recoverable

and potentially readable." It is unclear from this statement that the SAC team ever recovered and read any files. Further clarification is necessary in the same paragraph. If as stated in the report the drives were set up as a slave, the command would more appropriately read "d:\>list.txt" rather than "c:\>list.txt".

Findings and Recommendations

The Finding and Recommendation are built on the details contained in Attachment A. But the attachment is not entirely clear. Most specifically the "Comments" and "Location" columns field do not clearly indicate the warehouse location of the samples. From the attachment, the assumption is made that samples number 7 through 11 were the "loose" drives referred to on page 3 of the report. They include three of the five drives marked as degaussed but that had recoverable data. We also assume they had paper tape across the drive indicating these drives were degaussed, but it is not clear how they were labeled. If the samples 7 through 11 were physical hard drives laying on the shelves they would not have been sent to schools in that state. The school received only complete and bootable systems with the Windows 3x operating system. It is more likely that those drives would have been returned to FTC inventory and used in other agency equipment.

Of the remaining two drives that were marked as degaussed and had recoverable data, sample 14 had a comment of "drive not ready." In this case, it is likely that the technician was not able to access the drive because of the boot error and incorrectly labeled the drive as degaussed. Sample number 6 is unexplainable why it should of be marked degaussed and contain recoverable data other than human error.

Samples 12 and 18 from the label indicate these drives were prepared for re-use in other systems. The label "SID" typically indicates the drive was re-imaged with Window NT and at a sequence in the imaging process just prior to setting a unique system identifier. This is the first step in preparing a drive for use in a Windows NT configured PC. The label "C" is not meaningful and may only indicate it was a functioning boot drive.

Attachment B

Attachment B provides a sample of recoverable files. The auditors point out specific threats from the password list files and network configuration files. However, the passage of time has made that type of information much less useful. The password files are only relevant under Windows for Workgroups. The FTC has converted desktops to Windows NT and implemented a new password security policy that requires all staff to use "strong passwords" and change that password every 90 days. The network operating system enforces the policy. Therefore these file present only an extremely limited threat of unauthorized access to our computing environment.

Regarding the network configuration files, the network infrastructure has changed substantially with the introduction of new hardware at the end of calendar year 2000. The sub-netting scheme has been completely revised and any configuration information garnered from these Windows for Workgroup systems is obsolete.

Conclusion

We are in overall agreement with the conclusion of the report. ITM will review, update, and document the practices and procedures that are being followed to handle equipment and retrain all staff and contractors involved. However, Executive Order 12999 encourages agencies to make these donations and a change in policy would run counter to the spirit, if not the letter, of the order. We think it is appropriate to attempt to donate excess equipment to local schools, but also realize that, in most instances, that schools are not interested in the type of outdated equipment the FTC has available.

cc: Rosemarie Straight, Executive Director
Keith Golden, Associate CIO
Dennis Lynch, Assistant CIO for Litigation & Customer Support
Adam Trzeciak, OIG

OIG Response to Management Comments

On December 18, 2000, ITM management submitted to the OIG its comments to the audit report. (See memorandum from Chief Information Officer Richard Turner to Inspector General Fred Zirkel.) Management raised concerns about the OIG sample, its responsibilities under the *Computers for Learning Program*, and costs and vulnerabilities associated with implementing the program. An OIG discussion to these concerns is presented below.

Executive Order 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*, does not require agencies to excess computer equipment (PC's) to schools and other nonprofits, but rather provides management with the discretion to do so. Consequently, it is in the view of the OIG that participation in the program is a management decision and not a mandate.

While the program has many merits, we also noted that there are both monetary costs and security risks that should be considered. The impact on our financial resources is not fully known, as only three shipments have been made to local schools. However, we noted costs in the form of staff time to scrub the hard drives, load a new operating system, locate schools/nonprofits wanting outdated computers, transport the computers, and on occasion help the schools to set them up. ITM correctly pointed out that certain school districts in the metropolitan area (i.e., Fairfax County) have the technical expertise needed to support individual schools, and by implication, require little from the FTC in support services. Yet, from information provided to the OIG, FTC computers have gone only to Washington D.C. schools where technical support is needed. One D.C. school principal we spoke with said that technical expertise (to set up the computers) is as needed as the equipment itself. Given the age of many of the computers at the warehouse, we believe that more (not less) staff time will be needed to locate recipients for this equipment in the future.

Aside from the monetary costs to administer the program, the OIG was especially concerned that nonpublic/sensitive information could be contained on the hard drives of computers previously released to D.C. schools as well as those ready to be surplused out. We tested drives cleaned using the former "scrubbing" methodology (FDISK/FORMAT) to identify weaknesses in this prior method to determine whether nonpublic information was potentially released, as all computers released to date were scrubbed using this prior method. We do not imply, as stated on page 2 of your response, that these drives were ready for disbursal. Rather, we state on page 2 of the draft report that *it was recognized that FDISK/FORMAT alone would not be sufficient to make files unrecoverable, so the SOPHOS product and procedures were acquired and employed.* Further on page 5 we say that *the SACteam was informed that the Technology Operations team was in the process of using the SOPHOS purge software to clean the hard drives that were transferred to the warehouse prior to the implementation of the new practices.* We and the ITM staff recognized the shortcomings of the prior method and did not consider it secure.

As noted in the report, we found examples of "loose" drives and computers labeled "degaussed" (e.g., the new method) that had not been cleaned. We were told by ITM staff that the drives were ready to be reinstalled in computers that would eventually be donated. While it appeared that the new cleaning method did remove all data from the hard drives, we were concerned that controls to ensure that all computers were degaussed were not in place.

While outdated passwords and configuration files may no longer represent a serious threat to the agency's computer security given the recent security enhancements ITM has implemented, the OIG nevertheless was able to download documents (e.g., subpoenas, TRO's containing confidential company information, resumes, etc.) from "cleaned" and "degaussed" hard drives that are nonpublic no matter the age. We did not include the actual documents in the report for security and confidentiality reasons, but we will provide this information to you upon request.

The OIG appreciates your comments and have corrected the factual inaccuracies in our report.



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 24, 2001

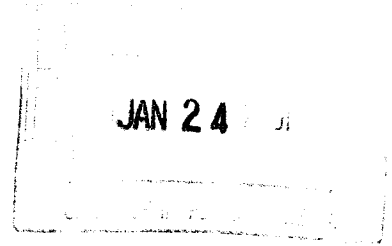
Memorandum

To: Fred Zirkel, Inspector General
Office of the Inspector General

From: Dennis M. Lynch *DML*
Assistant CIO for Litigation and Customer Support

thru Richard Turner *RT*
Chief Information Officer

Subject: Response to Recommendations Draft Audit Report Review of FTC Policies and Practices to Remove Sensitive Information from Surplused Hard Drives



This memorandum provides a response to recommendations provided as part of the draft audit AR01-049.

Recommendations

1. The report recommends ITM "Systematically re-examine the hard drive population" at the FTC warehouse. ITM will examine all drives currently designated as "Purged". "Degaussed" or otherwise denoted as ready for transfer to a suitable educational institute. ITM will verify that all drives are either rendered unusable or ensure the drives have been appropriately purged using an ITM copy of the Sophos Software.

Projected effort is:

Step	Description	Date*
1.	Freeze any effort to transfer equipment as donation to DC schools	done
2.	Develop specifications for warehouse re-examination effort	2/12/2001
3.	Acquire contract services to assist in re-examining hard drives stored in Alexandria warehouse	3/16/2001
4.	Start warehouse review effort	3/19/2001

5.	Periodically verify the work in progress	3/26/2001
6.	Complete re-examination effort	5/4/2001
7.	Finally verification of work	5/11/2001

2, The report recommends ITM “develop formal procedures for removal of sensitive information from hard drives and establish a stronger control structure.” ITM will develop formal procedures, document those procedures, train contractor support staff, and monitor implementation of those procedures. ITM will conduct an interim audit, monitor contractor support staff compliance with procedures and evaluate the effectiveness of those procedures. ITM will develop a stronger control structure by assigning ITM staff with the responsibility of verifying the performance of the contractor support staff by sampling every batch of computer drives scheduled for surplus.

Projected effort is:

Step	Description	Date*
1.	Develop initial draft of procedures	3/2/2001
2.	Review draft with technical contractor support staff	3/6/2001
3.	Incorporate comments	3/13/2001
4.	Implement procedures	3/19/2001
5.	Assign government staff to perform periodic reviews	3/19/2001
6.	Conduct management assessment with technical contractor support staff input on the new procedures	5/11/2001

3. The report recommends ITM “establish procedures for periodically examining computers at the warehouse”. ITM will establish procedures that will recommend that all drives be removed from PCs prior to shipment to the warehouse. The drives will be purged at the headquarter’s building, stored and secured separately from the PC . In the event drives are moved to the warehouse or some other off-site location ITM staff will verify that the degaussing process was managed appropriately by the contractor technical operations staff through a random check of these specific drives. Independently, ITM staff will periodically examine drives stored at headquarters to verify effective destruction of electron information on excess drives and review compliance with established procedures.

Projected effort is:

Step	Description	Date*
1.	ITM will conduct periodic reviews of drives	3/2/2001
2.	ITM will sample drives prior to transfer to any outside entity	ongoing

4. The report suggests ITM consider whether there “may be a benefit to following up with outside recipients of surplus FTC computers”. Given the reservations noted in the report, the elapsed time and the departure of key personnel involved in the original transfer, ITM suggests we do not follow-up on this recommendation.

* Please note that dates are based on the current date of this memo.

cc: Keith Golden
Associate CIO for Information and Technology Management

Adam R. Trzeciak, Audit Manager
Office of Inspector General