November 21, 2016

MEMORANDUM

TO: Paul Wiedefeld
General Manager

FROM: Helen Lew ***/s/***
Inspector General

SUBJECT: Degaussing/Wiping of Electronic and Magnetic Media (OIG-17-03)

The purpose of this Final Memorandum Audit Report is to bring to your attention security weaknesses in the Washington Metropolitan Area Transit Authority's (WMATA) processes for degaussing/wiping electronic and magnetic media and the quality assurance processes designed to detect the effectiveness of the processes. Specifically, hard drives that were available for public auction had not been erased. These hard drives contained WMATA business data and user personally identifiable information (PII), which in the wrong hands, could be used for other than legitimate purposes.

Washington
Metropolitan Area
Transit Authority

cc: CFO - D. Anosike
IBOP - J. Kuo
COUN - P. Lee

[redacted]

Background

During the Office of Inspector General's (OIG) *Audit of WMATA's Mobile Computing Security Program*, it came to our attention WMATA had not securely erased two personal computer (PC) hard drives. While this observation was outside the scope of the mobile computing audit, it is similar to a finding identified in a May 25, 2012 OIG report.[1] That report provides there was "inadequate verification of data removed from computer hard drives prior to public auction." Specifically, storage media was not being securely erased prior to the media being surplused. The repeat discovery of this condition suggests weak information technology security controls.

What is Required

Magnetic Media Erasure Requirements - Policy Instruction (P/I) 15/12.1, section 5.07(a) provides "[e]lectronic and magnetic media (e.g., hard drives, diskettes, magnetic tapes and optical tapes) should be erased using secure deletion tools before transfer or disposal." Also, the Department of Information Technology, Department of Data Center & Infrastructure, IT Customer Support Services, *Degaussing/Wiping Hard Drives Standard Operating Procedures* dated June 6, 2012, (Degaussing SOP), page 4, provides " . . . procedures for permanently erasing (degaussing/wiping) electronic data from Washington Metropolitan Area Transit Authority (WMATA) IT equipment (PCs, laptops and other IT assets) prior to surplussing the equipment . . . ."

Quality Assurance/Audit Requirements - The Degaussing SOP, Step 5 provides "Once each month, the Chief of Data Center and Infrastructure requests a WMATA employee who does not work in DCI Inventory to audit the degaussing/wiping procedures. These audits are intended to enable IT to confirm that its degaussing/wiping procedures remain effective." Specifically, the auditor randomly selects a minimum of four recently degaussed hard drives each month to ". . . test and confirm that each drive is completely unusable" and four recently wiped hard drives to ". . . test and confirm that each drive is blank and ready for re-use."

[1] OIG report entitled Review of WMATA's Software/Hardware Acquisition Process, (IT 12-002), dated May 25, 2012.

[redacted]

What We Found

We selected two PC hard drives that had been transferred to Open Material Storage (OMS) Facility and were available for public auction. One hard drive contained 2,326 files, 196 subfolders, and tax software. The second hard drive contained 2,783 files within 192 subfolders. Both hard drives contained PII, such as the names of 19 previous users.

For the two hard drives examined, the Department of Rail Services did not send the hard drives to the IT Department for secure erasure prior to them being transferred to the OMS Facility. As such, the Department of Rail Services circumvented controls to ensure secure erasure of storage media prior to disposal or transfer. The Investment Recovery Administrator at the OMS Facility stated any WMATA employee can surplus equipment as long as they have the corresponding Property Transfer Request form. This process could also lead to circumvention of controls intended to ensure hard drives are erased prior to disposal or transfer. DCI Officials stated they do not erase server hard drives. However, according to the P/I 15.12 and Degaussing SOP, the IT Department should erase all electronic and magnetic media.

Additionally, the IT Department could not provide documentation to demonstrate the department conducted the monthly audits.

Why this is Important?

Failing to remove data from storage media prior to its transfer or disposal, increases the risk that critical and sensitive business data stored on storage media may be compromised and used for other than legitimate purposes.

[redacted]

Recommendations

We recommend the GM/CEO:

1. Develop and implement security controls and processes to allow: (1) only authorized custodians to surplus equipment, and (2) surplus facilities to only accept electronic storage media the IT Department has certified as securely erased. (Action: Chief of Internal Business Operations) (Risk-High)[2]

2. Identify, assign and train staff to conduct the monthly audits required by the Degaussing SOP. (Action: Chief of Internal Business Operations) (Risk-Medium) [3]

Agency Comments

WMATA provided written comments to this report on November 10, 2016, (see Appendix). The Chief of Internal Business Operations fully concurred with our finding and recommendations and agreed to implement internal controls and take appropriate corrective actions. Further, the Chief of Internal Business Operations agreed to take actions to ensure electronic storage media that resides at OMS Facility is securely erased.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG follow-up.

Scope and Methodology

This audit focused on evaluating WMATA's cleaning of electronic media (hard drives) prior to their disposal and is a follow-up to OIG report entitled *Audit of WMATA's Software/Hardware Acquisition Process* (IT-12-002), dated May 25, 2012. We conducted this performance audit in August 2016. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, the auditors were aware of the possibility of fraud, waste, or abuse in the program.

[2]High – Exception is material to accomplishing organization objectives. Corrective action by appropriate Senior Management is required. Resolution would help avoid loss of material assets, reputation, critical financial information or ability to comply with critical laws, policies, or procedures.

[3]Medium – Exception may be material to accomplishing organization objectives. Corrective action is required and the results are reported to management quarterly. Resolution would help avoid negative impact on the unit's assets, financial information, or ability to comply with important laws, policies, or procedures.

[redacted]

To address the audit objective, OIG auditors reviewed relevant documents, including WMATA policy instructions and office procedures. Several related internal communication documents pertaining to the audit were also reviewed. Additionally, OIG auditors conducted interviews with WMATA staff to obtain further information and insights on the processes used to dispose of electronic media that was no longer needed. We randomly selected two PC hard drives at the OMS Facility and conducted tests to determine whether these hard drives contained data.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards required that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[redacted]

Appendix

M E M O R A N D U M

SUBJECT: Response to Evaluation Report OIG-17-003 Degaussing/Wiping of Electronic and Magnetic Media

DATE: November 10, 2016

FROM: AGM IT/CIO - Kevin Borek [redacted]

THRU: CIBO - John Ku [redacted]

TO: GM/CEO – Paul Wiedefeld [redacted]

The following represents the Chief Information Officer's Corrective Action Plan (CAP) in response to OIG's *Evaluation Report of WMATA's Degaussing/Wiping of Electronic and Magnetic Media*. Our responses to the recommendations and our planned actions are outlined below:

OIG Recommendation One:
Develop and implement security controls and processes to allow: (1) only authorized custodians to surplus equipment, and (2) surplus facilities to only accept electronic storage media the IT Department has certified as securely erased.

IT's Response:
IT accepts this recommendation. As noted in the audit, the hard drives in question were not sent to IT for secure erasure, circumventing an existing policy and process.

IT will be updating its policies to strengthen and explicitly clarify that electronic media must be sent to IT-DCI for secure wiping prior to submission to surplus facilities. In addition, IT will be requesting all electronic storage equipment currently in surplus at OMS that has not been provided by IT be sent to IT-DCI for secure wiping.

IT will complete these tasks by *November 1, 2017*.

Recommendation Two:
Identify, assign and train staff to conduct the monthly audits required by the Degaussing SOP

Washington Metropolitan Area Transit Authority

IT's Response:
IT accepts this recommendation. We will updating our Degaussing SOP to strengthen our processes and further clarify verbiage outlining actions that are required by managers to conduct monthly audits.

IT will complete these tasks by *November 1, 2017*.