Description of document:	Washington Metropolitan Area Transit Authority (WMATA) Office of the Inspector General (OIG) Management Alerts/Advisories 2016-2022
Requested date:	13-May-2022
Release date:	13-December-2024
Posted date:	06-January-2025
Source of document:	Office of General Counsel 7E Washington Metropolitan Area Transit Authority P.O. Box 44390 Washington, DC 20026-4390 Attention: PARP Administrator Fax: (202) 962-2550 Email: PARP@wmata.com

From: Yanos, Brian J. <bjyanos@wmata.com>
Cc: Rashbaum, Benjamin <brashbaum@wmata.com>; Noh, Richard D. <rdnoh@wmata.com>
Sent: Friday, December 13, 2024 at 02:30:33 PM EST
Subject: PARP Request 22-0117; OIG Management Alerts/Management Advisory Documents 1.1.2012 to Present

This is the Washington Metropolitan Area Transit Authority's (WMATA) final decision in response to your May 13, 2022, Public Access to Records Policy (PARP) request for "each WMATA OIG 'Management Alert' or 'Management Advisory' document during the timeframe January 1, 2012 to the present."[1]

Your request was processed pursuant to WMATA's PARP.[2]

On September 7, 2022, you emailed us that you: "narrow[ed your] request to whatever OIG Management Alerts and OIG Management Advisories are retrievable within a 2.5 hour timeframe."

Decision

The following OIG Management Alerts & Assistance Reports can be located online:

Results of Core Testing for Concrete Panels Silver Line Phase 2 (MA-20-0001) 8-16-19

https://wmataoig.gov/wp-content/uploads/2021/06/Management-Alert-Results-of-Core-Testing-for-Concrete-Panels-Silver-Line-Phase-2.pdf

Track Ballast - Rail Yard Silver Line Phase 2 (MA-20-0002) 8-19-19

https://wmataoig.gov/wp-content/uploads/2021/06/Management-Alert-Track-Ballast-Rail-Yard-Silver-Line-Phase-2.pdf

In addition, please find attached the following record responsive to your request (78 pages total):

OIG Management Alerts & Assistance Reports 10-13-16 to 4-5-22[3]

Pursuant to PARP Exemption 6.1.1 (sensitive security information/critical infrastructure information), we redacted information that could pose a risk to the safety and security of WMATA's system, passengers, or employees if released.

Pursuant to PARP Exemption 6.1.4 (confidential commercial information), we redacted portions of the records responsive to your request for submitted responses of all proposers because the contractor has identified these portions as containing information that the contractor actually and customarily treats as confidential.

Pursuant to PARP Exemption 6.1.5 (deliberative process privilege & self-evaluative privilege), we redacted observations, evaluations, and determinations that were issued to help WMATA make a final decision.

Pursuant to PARP Exemption 6.1.6 (personal privacy), we redacted personal information of individuals whose privacy interests outweigh the public interest in disclosure.

After a search reasonably calculated to find all relevant records, WMATA has found no additional records responsive to your request.[4]

Appeal Rights

If you wish to appeal WMATA's decision, in accordance with PARP § 9.1, you may file a written appeal of the action with the Executive Vice President, External Relations (or designee) at PARP_Appeal@wmata.com, within 30 business days of the date of this decision letter. Further details about our appeals process can be found on our website.

Future correspondence should reference the request number noted in the subject line of this correspondence. If you have any questions, please contact me, if I am unavailable, you may contact Benjamin Rashbaum at BRashbaum@wmata.com or 202-962-1926.

Sincerely,
Brian Yanos

[1] The date that WMATA started the search for records responsive to this request, in this case, May 19, 2022, is established as the cut-off date for this request.

2 The PARP can be found on WMATA's website at https://www.wmata.com/about/records/public-records.cfm, under the section marked "Legal Affairs."

3 Pages 34-38 contain pre-existing redactions as WMATA is unable to locate a non-redacted version of this record. Therefore, it is being provided with the pre-existing redactions as well as additional redactions labeled as PARP exemptions.

4 WMATA's Office of the Inspector General started using Management Alerts and Management Assistance Reports in 2016.

Brian J. Yanos
PARP Attorney, Associate Counsel
Legal & Compliance
202-627-4542

This transmission is intended only for the proper recipient(s). It is confidential and may contain attorney-client privileged information or information prepared in anticipation of litigation. If you are not the proper recipient, please notify the sender immediately and delete this message. Any unauthorized review, copying, or use of this message is prohibited.

[1] The date that WMATA started the search for records responsive to this request, in this case, May 19, 2022, is established as the cut-off date for this request.

[2] The PARP can be found on WMATA's website at https://www.wmata.com/about/records/public-records.cfm, under the section marked "Legal Affairs."

[3] Pages 34-38 contain pre-existing redactions as WMATA is unable to locate a non-redacted version of this record. Therefore, it is being provided with the pre-existing redactions as well as additional redactions labeled as PARP exemptions.

[4] WMATA's Office of the Inspector General started using Management Alerts and Management Assistance Reports in 2016.

M E M O R A N D U M

MANAGEMENT ALERT REPORT
(INVESTIGATION NO. 16-0019-I)

SUBJECT: Transmission of WMATA Data to An Unsecured Personal Email Account

DATE: October 13, 2016

FROM: OIG – Helen Lew

TO: GMGR – Paul Wiedefeld

Issue

OIG determined that PARP Ex. 6.1.6 transmitted WMATA data to an unsecured personal e-mail account. The utilization of a personal e-mail account to conduct WMATA business and sending WMATA business information to a personal e-mail account are violations of WMATA's Policy/Instruction (P/I) 15.3/3 *Electronic Access Usage Policy.* Further, the transmission of WMATA business information to an unsecured device presents a significant threat to information security in the event of theft or loss. This threat is increased given the nature of information processed by PARP Ex. 6.1.6, which may contain personally identifiable information.

Background

During the course of an investigation, the Office of Inspector General (OIG) discovered PARP Ex. 6.1.6 routinely utilized a personal computer in the course of conducting WMATA business. According to PARP Ex. 6.1.6 personal laptop contained a significant amount of PARP Ex. 6.1.6 industry data and trends. PARP Ex. 6.1.6 said PARP Ex. 6.1.6 often keeps PARP Ex. 6.1.6 personal laptop readily available at work to compare current WMATA practices to the data stored on PARP Ex. 6.1.6 laptop.

PARP Ex. 6.1.6 further stated PARP Ex. 6.1.6 responsibilities as PARP Ex. 6.1.6 frequently require PARP Ex. 6.1.6 to take work home. PARP Ex. 6.1.6 said PARP Ex. 6.1.6 e-mails WMATA information to PARP Ex. 6.1.6 personal e-mail account, which PARP Ex. 6.1.6 then downloads onto PARP Ex. 6.1.6 personal computer. This allows PARP Ex. 6.1.6 to continue to work during PARP Ex. 6.1.6 commute and at home when PARP Ex. 6.1.6 internet connectivity is unreliable. PARP Ex. 6.1.6 confirmed the e-mails and documents downloaded to PARP Ex. 6.1.6 personal computer are neither password protected nor encrypted.

When asked by OIG, PARP Ex. 6.1.6 stated PARP Ex. 6.1.6 was not familiar with WMATA's policy on storing and accessing WMATA data, P/I 15.3/3. PARP Ex. 6.1.6 was presented a copy of P/I 15.3/3 and reviewed §5.02(l) and (m) which identified sending WMATA material to a personal e-mail account and using personal e-mail for WMATA business as inappropriate usage.

Washington Metropolitan Area Transit Authority

Recommendations

The security of WMATA business data, including but not limited to personally identifiable information, is an integral part of efficient and effective operations. As such, OIG recommends the following:

1. IT should ensure all supervisors and managers within WMATA are familiar with P/I 15.3/3, with specific emphasis on what activity is considered inappropriate electronic access/usage.

2. [redacted] should be instructed to immediately cease transmitting WMATA data to [redacted] personal e-mail account.

3. [redacted] should be instructed to utilize either [redacted] WMATA issued laptop or WMATA's Virtual Private Network for conducting WMATA business.

M E M O R A N D U M

MANAGEMENT ALERT REPORT (Purchase Card Program)

SUBJECT: Purchase Card Program Concerns DATE: March 17, 2017

FROM: OIG – Helen Lew

TO: GMGR – Paul Wiedefeld

WMATA's Purchase Card Program provides designated personnel a simplified acquisition method for procuring items and services at or below $3,500 in accordance with procurement policy. In 2016, WMATA's 194 authorized cardholders accrued $15,240,109 in purchase card expenditures.

The Purchase Card Program is subject to significantly fewer internal controls and oversight mechanisms when compared to other procurement methods, making for an environment that is especially susceptible to waste, fraud, and abuse. OIG has identified a litany of concerning purchase card practices across multiple WMATA departments during the course of both recently completed and ongoing investigations. Most notably, OIG has identified patterns of (1) fraudulent transactions for personal gain, (2) frivolous or highly questionable expenditures, and (3) violations and circumvention of purchase card/procurement policy. Similarities observed in multiple departments suggest the possibility these concerning practices may be prevalent Authority-wide. OIG believes improving controls and oversight mechanisms in this area may also offer significant opportunity for cost savings in the current fiscal environment.

Washington Metropolitan Area Transit Authority

Background

WMATA-issued purchase cards may be used as a simplified method for filling anticipated repetitive needs for supplies, services, or other items. WMATA's purchase card policy allows for authorized employees to purchase commercially available goods and services at or below $3,500. Purchase cards can also be used for orders against established contracts or purchase orders up to the $150,000 simplified acquisition threshold. The policy states cardholders hold a public trust and shall use the purchase card for official business purposes only and in strict accordance with the Procurement Procedures Manual (PPM) and Standards of Conduct.

Purchase card transactions are to be strictly monitored by the cardholder and the cardholder's approving official for adherence to these policies. In addition, the cardholder is required to maintain supporting documentation

for all transactions for a three-year period. The Office of Procurement and Materials (PRMT) provides training for cardholders and approving officials before purchase card authority is delegated, as well as refresher training for cardholders and approving officials on an annual basis thereafter.
PRMT has PARP Ex. 6.1.6 responsible for administering the Purchase Card Program and monitoring cardholder transactions. PARP Ex. 6.1.6 has been an asset to OIG by both alerting the office to potential waste, fraud, and abuse and being responsive to investigative needs. However, despite PARP Ex. 6 assistance, it is apparent that PARP Ex. 6 cannot provide the level of scrutiny needed to maintain the integrity of the program alone.

In PARP Ex. 6.1.6 2016, OIG's report of investigation (ROI) PARP Ex. 6.1.6 detailed significant issues with PARP Ex. 6.1.6 procurement practices, especially as they pertained to the use of purchase cards and blanket purchase agreements. PARP Ex. 6.1.6 management was found to have exercised poor judgment in managing and monitoring the purchase card expenditures of subordinates, and PARP Ex. 6.1.6 used PARP Ex. purchase card in a wasteful and, in some instances, fraudulent manner.

Developments in ongoing OIG investigations have revealed numerous concerning purchase card practices; many of which are similar in nature to those identified in ROI PARP Ex. 6.1.6. Most notably, OIG has identified similarities with respect to (1) fraudulent transactions for personal gain, (2) frivolous or highly questionable expenditures, and (3) violations and circumvention of purchase card/procurement policy. Each area of concern is discussed in detail below.

Fraudulent Transactions for Personal Gain
ROI 15-0012-I identified examples of PARP Ex. 6.1.6 using PARP Ex purchase card to steer WMATA business to benefit outside interests. This included using PARP Ex. 6 purchase card to procure services from friends, family members, and WMATA colleagues. These actions were clear violations of not only purchase card policy, but also conflict of interest provisions of WMATA's Compact (Article III, Section 10), WMATAs Ethics Policy, and the PPM Standards of Conduct (2-10). OIG also found some invoices used for services provided by an associate of PARP Ex. 6.1.6 were fabricated in order to process purchase card payments.

In PARP Ex. 6.1.6 2015, OIG conducted a purchase card investigation pertaining to PARP Ex. 6.1.6 .[1] PARP Ex. 6.1.6 are alleged to have used two

[1] OIG case PARP Ex. 6.1.6

purchase cards to engage in a fraudulent scheme which involved recurring, high-dollar transactions with fictitious companies for cleaning products that were never received by WMATA. This investigation was turned over to the Federal Bureau of Investigations (FBI) and PARP Ex. 6.1.6 personnel were terminated as a result, and losses to WMATA were estimated to be over $400,000.

More recently, OIG has initiated an investigation into personnel suspected of using a purchase card to procure miscellaneous PARP Ex. 6.1.6 to construct personal items during WMATA work hours for managers and employees of other departments. Though not yet confirmed, OIG received preliminary information materials procured with the purchase card have been used to PARP Ex. 6.1.6 This investigation, though still ongoing, also has potential criminal implications.

Frivolous or Highly Questionable Expenditures

During the course of the above mentioned investigations, OIG has identified a large number of frivolous or highly questionable expenditures. OIG does not necessarily consider these types of expenditures to be fraudulent in nature, though some clearly appear to be wasteful and an abuse of resources considering the quantity purchased. Frivolous expenditures observed within the departments investigated include:

PARP Ex. 6.1.6

OIG noted, with the exception of the PARP Ex. 6.1.6 purchase, all frivolous expenditures above were made at the direction of a senior manager in that department.

Some of the expenditures identified by OIG may appear to be for a justifiable business need. OIG notes, however, in the absence of proper controls and

[2]Asterisk (*) indicates expenditure was observed at multiple departments.

[3]The PARP Ex. 6 employee responsible for this purchase PARP Ex. 6.1.6.

oversight, expenditures for these items and services can be manipulated for personal use with relative ease. As such, OIG believes the purchase card may not be the most appropriate procurement method for these expenditures. Examples of expenditure types observed during investigations include:

- Office facility repair/renovation/demolition work*
- Painting services
- Maintenance/repair work for WMATA leased vehicles
- Signs for WMATA facilities/work activities*
- Electronics*
- Home improvement supplies*
- Scanning and lamination services

OIG notes WMATA may have in-house resources or capabilities to provide some of the above items/services at better cost. In most cases OIG found this was not considered by the cardholder or department management responsible for directing the expenditure.

Violations and Circumvention of Purchase Card/Procurement Policy

OIG observed numerous violations of purchase card policy while investigating the above mentioned departments, which indicates both a disregard for said policy and a breakdown of oversight and enforcement.

Policy requires cardholders to upload transaction-related information and supporting documentation into Citigroup's[4] online Card Management System. OIG observed the cardholders investigated often entered blank or insufficiently detailed expenditure descriptions. In some cases cardholder reconciliation and approving official review were not done in a timely manner, or at all, in the system as required.

OIG observed cardholders investigated had little to no supporting documentation for any of their purchase card transactions, despite the requirement to maintain such documentation in hardcopy for three years. OIG also identified numerous split purchases[5] and examples of purchase cards being used to procure items or services for which there was already an established contract. Both behaviors are prohibited by policy.

In addition, cardholders from all departments had examples of recurring or routinely used services that cost over $150,000 in aggregate which, by policy, should have been placed on a competitive contract. In at least one instance, a cardholder was allowed to increase the credit limit on his purchase card to

[4]WMATA's purchase card provider.

[5]Defined by policy as "A known requirement split into multiple transactions to circumvent the single purchase limit," which also states, "Split purchases are strictly prohibited."

continue making these purchases in high volume instead of being instructed to use a more conventional contract. OIG believes this to be an inappropriate circumvention of policy, which limits competition and potential cost-efficiencies.

In one department, OIG learned purchase card expenditures were being used to supplement Capital Improvement Program (CIP) funded work activities and construction work under a job order contract (JOC). OIG believes this to be a potentially inappropriate circumvention of the procurement policy associated with each of those contract vehicles.

Especially concerning was information indicating some cardholders are not properly securing their purchase cards. Purchase card policy states the following (P/I 8.11/1 – 7.06):

> *The Cardholder shall safeguard their purchase card and account number at all times and shall keep them in a secure location. The only person allowed to use the card is the Cardholder whose name appears on the card. Cardholders shall not allow anyone…to use their card or account number. Cardholders shall not save their purchase card number into a merchant's internet website for future purchases…"*

Based on information obtained, OIG believes some cardholders may not be properly securing the purchase card and the corresponding account numbers. This increases the potential for fraud, waste, and abuse. OIG was informed one cardholder in particular regularly allows multiple subordinates to take physical possession of [redacted] purchase card for purchasing work materials.

Inventory and Asset Management Concerns

OIG is aware inventory control and asset management are an Executive Leadership priority. The use of purchase card transactions to circumvent conventional contracts has a tangential effect on inventory management at the local department level. As an example, OIG became aware of multiple storage areas maintained locally by offices within departments under investigation. These storage areas appear to operate outside [redacted] supervision, and may not have appropriate inventory and asset management controls in place to prevent fraud, waste, and abuse.

OIG has observed many purchase card expenditures with home improvement supply retailers, such as [redacted]. Even with supporting documentation, due to the job responsibilities of many

operations personnel, OIG cannot reliably determine whether these expenditures are being used for work or personal use.

For example, one of OIG's ongoing investigations suggests materials procured via purchase card are being stored in a storage area that is accessible to all office personnel. OIG has been told no inventory method to track incoming/outgoing materials is in use, and materials are alleged to have gone missing or to have been used for personal projects.

Materials that are purchased via purchase card and maintained in these independent storage areas are highly susceptible to theft, loss, and redundant purchasing.

Recommendations

Despite clear purchase card policy and procedures, OIG has observed blatant violations and questionable spending patterns which are of concern. Based on findings from both previous and ongoing investigations, OIG recommends the following actions be taken:

1. Management should consider whether the Purchase Card Program has adequate resources to effectively execute its oversight role and commensurate authority to enforce corrective actions for non-compliance.

2. The Office of Procurement and Materials (PRMT) should reassess whether the number of cardholders Authority-wide and the credit limits afforded to each cardholder are appropriate in the current fiscal environment.

3. The Office of Quality and Internal Compliance Operations should be tasked with conducting a more comprehensive review of the Purchase Card Program with a specific focus on the appropriateness of expenditures being made within departments.

4. PRMT issue guidance on the appropriateness of the expenditure categories identified by OIG above and through QICO's subsequent review.

REPORT OF INVESTIGATION

Complaint No.: 17-0021-I (**Purchase Card Misuse**)

Date: August 14, 2017

Executive Summary

OIG received an allegation that PARP Ex. 6.1.6 gave PARP Ex. 6.1.6 WMATA issued Purchase Card to PARP Ex. 6.1.6 to make purchases for both WMATA and personal use. Additionally, it was alleged PARP Ex. 6.1.6 Further, it was purported PARP Ex. 6.1.6 had PARP Ex. 6.1.6 outside of WMATA business hours, in exchange for PARP Ex. 6.1.6.

The allegations were substantiated in part. The investigation determined PARP Ex. 6.1.6 provided PARP Ex. 6.1.6 Purchase Card to several WMATA employees, for them to conduct transactions with multiple vendors. Further, the investigation revealed PARP Ex. 6.1.6 did not safeguard WMATA supplies to prevent employees from freely taking them from the PARP Ex. 6.1.6, and according to multiple witnesses, PARP Ex. 6.1.6 directed the completion of several "off the books" projects. Finally, OIG did not uncover any evidence that PARP Ex. 6.1.6 exchanged beneficial treatment for PARP Ex. 6.1.6 outside of WMATA.

Although PARP Ex. 6.1.6 was one of several Purchase Card holders within PARP Ex. 6.1.6 was responsible for PARP Ex. 6.1.6 of the purchases for the entire division.[1] A detailed analysis of PARP Ex. 6.1.6 Purchase Card transactions uncovered that 46% of PARP Ex. 6.1.6 transactions could not be justified under the standards imposed by the Purchase Card Policy.[2]

OIG interviewed PARP Ex. 6.1.6 regarding the allegations. Subsequent inquiry revealed PARP Ex. 6.1.6 provided several false and misleading statements to OIG with regards to PARP Ex. 6.1.6 Purchase Card use and the inventory controls PARP Ex. 6.1.6 imposed within PARP Ex. 6.1.6 division.

---

[1] From PARP Ex. 6.1.6 2016 to PARP Ex. 6.1.6 2017.

[2] P/I 8.11/1 Purchase Card Policy

Summary of Investigation

The OIG investigation into the allegation uncovered three main areas of concern:

- Purchase Card misuse by PARP Ex. 6.1.6
- Improper inventory controls for the PARP Ex. 6.1.6 located at PARP Ex. 6
- PARP Ex. 6.1.6 false statements to OIG

Purchase Card Misuse

The OIG investigation determined PARP Ex. 6.1.6 failed to maintain the security of PARP E Purchase Card and account information. OIG obtained the receipts for PARP Ex. 6.1.6 Purchase Card transactions from PARP Ex. 6.1.6 2016 to PARP Ex. 6.1.6 2017. The signatures on these receipts were drastically different, and on some occasions, the WMATA employee signed their own name instead of PARP Ex. 6.1.6. The allegation that PARP Ex. 6.1.6 allowed PARP Ex. 6.1.6 to utilize PARP E Purchase Card was further verified through several interviews of PARP Ex. 6.1.6 personnel.

This lack of control over the physical Purchase Card likely contributed to the failure of PARP Ex. 6.1.6 to maintain the proper records for the Purchase Card purchases. All witnesses indicated there was a severe inventory problem for PARP Ex. 6.1.6. All of the PARP Ex. 6.1.6 and PARP Ex. 6.1.6 interviewed by OIG indicated WMATA storerooms did not maintain the proper inventory of the supplies used on a daily basis, and therefore, PARP Ex. 6.1.6 Purchase Card was used to supplement the in-house inventory for the PARP Ex. 6.1.6. The purchase of inventory items with the Purchase Card is prohibited unless there is a "no stock" condition system-wide.[3] To justify utilizing the Purchase Card for inventory items, the Cardholder must provide a copy of the receipt, along with the WMATA stock number, to the Stock Clerk within five days. The Clerk then inputs the need for resupply into the Maximo system. None of PARP Ex. 6.1.6 receipts included a WMATA stock number, nor did PARP Ex. 6.1.6 forward the receipts to the Stock Clerk to address the lack of inventory. The witnesses interviewed by OIG indicated frustration with the Maximo storeroom system, and this frustration led to the use of PARP Ex. 6.1.6 Purchase Card as a default for supplies, rather than utilizing WMATA storerooms.

While OIG found three Blanket Purchase Agreements (BPAs) in place for PARP Ex. 6.1.6[4], none of the witnesses interviewed were aware these procurement vehicles were in place. As a result, all supplies for PARP Ex. 6.1.6 that were not obtained through WMATA storerooms were purchased on the Purchase Cards. The investigation revealed that PARP Ex. 6.1.6 spent PARP Ex. 6.1.6 on PARP Ex. 6.1.6 instead of utilizing the BPA in place for these purchases.[5]

The investigation also revealed PARP Ex. 6.1.6 failed to provide valid Maximo Work Order numbers to justify all of PARP E Purchase Card transactions. OIG found PARP transactions totaling PARP Ex. 6.1.6, where PARP Ex. 6.1.6 either provided a work order number that did not correspond with

[3] P/I 8.11/1 Purchase Card Policy, section 13.03.

[4] BPAs were for PARP Ex. 6.1.6.

[5] See Exhibit 1 and Exhibit 2.

any work order ticket within the PARP Ex. 6.1.6 system, or PARP E failed to provide a PARP Ex. 6.1.6 work order number all together.[6]

For those purchases where PARP Ex. 6.1.6 provided a valid work order number, OIG compared the itemized receipt and PARP Ex. 6.1.6 expense report description, to the description provided in PARP Ex. 6.1.6, as well as any notes provided by the PARP Ex. 6.1.6 assigned to that ticket. This uncovered PARP E occasions totaling PARP Ex. 6.1.6 where items purchased were not justified by the records.[7] These records corroborated witness statements that PARP Ex. 6.1.6 does not control the use of PARP Ex. Purchase Card. Witnesses indicated PARP Ex. 6.1.6 collects the receipts after PARP E directs a subordinate to use PARP E Purchase Card, but PARP E does not verify whether the purchases were justified. One witness admitted there were many instances were a work order ticket was cancelled, and supplies were still purchased for the cancelled job, or there were duplicate purchases made due to a lack of communication between PARP Ex. 6.1.6 and the assigned PARP Ex. 6.1.6. Multiple witnesses indicated these "extra" purchases are stored on the PARP Ex. 6.1.6 until they "disappear." Witnesses indicated this occurs through employees taking the items, and one witness stated some items are thrown out if their presence on PARP Ex. 6.1.6 becomes too conspicuous (e.g. too many PARP Ex. 6.1.6 on the PARP Ex. 6.1.6 that have no paperwork for installation).

PARP Ex. 6.1.6 admitted PARP E created a "generic" work order in PARP Ex. 6.1.6 that PARP E assigns when the purchase was to maintain inventory within the PARP Ex. 6.1.6, or if the purchase was for another supervisor within PARP Ex. 6.1.6 who did not provide PARP Ex. with a PARP Ex. 6.1.6 work order number to justify the purchase. The investigation determined PARP Ex. 6.1.6 listed a generic work order number as the justification for PARP Ex. 6.1.6 or 36% of PARP E total Purchase Card transactions.[8]

Finally, OIG uncovered PAR instances where PARP Ex. 6.1.6 conducted split purchases to avoid the $3,500 single purchase limit imposed on Cardholders. All three split purchases were for PARP Ex. 6.1.6 purchased through the same vendor, PARP Ex. 6.1.4

Improper Inventory Controls

The investigation found PARP Ex. 6.1.6 failed to maintain any inventory controls or proper security at the PARP Ex. 6.1.6. While the PARP Ex. 6.1.6 has a gate to restrict access, witnesses indicated these gates are not always closed or locked. This was verified by an unannounced OIG PARP Ex. 6.1 visit, where the PARP Ex. 6.1.6 was open despite all employees being at lunch. All witnesses, with the exception of PARP Ex. 6.1.6 (see below), indicated there were no controls or monitoring of the PARP Ex. 6.1.6 inventory. There is no inventory log for the items received from WMATA storerooms or through Purchase Card transactions. Additionally,

[6] See Exhibit 3.
[7] See Exhibit 4.
[8] See Exhibit 5.

there is no inventory log for the multiple PARP Ex. 6.1.6 utilized by the PARP Ex. 6.1.6. No one is required to justify the need for any item before it is removed from the PARP Ex. 6.1.6 The PARP Ex. 6.1.6 are not required to update the PARP Ex. 6.1.6 record with the supplies or tools they used to complete the work order task.

This lack of controls has resulted in the abuse of the PARP Ex. 6.1.6 inventory. Multiple witnesses indicated the PARP Ex. 6.1.6 is seen as a "candy shop" where any WMATA employee can freely take supplies without documentation or justification. Multiple witnesses indicated it was not unusual for PARP Ex. 6.1.6 from other locations to use supplies from the PARP Ex. 6.1.6 to complete their projects. Due to the complete lack of any inventory log or documentation of what supplies are used for each project, there is no means to track whether the supplies taken from the PARP Ex. 6.1.6 are used for legitimate WMATA projects or personal use.

The lack of inventory controls has also led to several "off the books" projects. All of the PARP Ex. 6.1.6 interviewed stated they regularly complete additional "small requests" that are made once they respond to a Work Order ticket. These smaller projects are completed without the creation of a separate Work Order. Additionally, several witnesses corroborated the complainant's allegation that PARP Ex. 6.1.6 were directed by PARP Ex. 6.1.6 to complete larger projects, such as building PARP Ex. 6.1.6, without any PARP Ex. 6.1.6 work order ticket or documentation. The witnesses indicated these projects are completed during regular work hours, using WMATA supplies. Any purchases made for these projects, and any time spent to complete them, was ascribed to the generic PARP Ex. 6.1.6 ticket in PARP Ex. 6.1.6. The witnesses interviewed by OIG could not verify if these larger projects were for in-office or at home personal use. OIG obtained a photo that was identified as a PARP Ex. 6.1.6 built for one of these "off the books" projects.[9] The PARP Ex. 6.1.6 is loaded on what was identified as PARP Ex. 6.1.6 personal vehicle. PARP Ex. 6.1.6 stated the PARP Ex. 6.1.6 was for PARP Ex. 6.1.6, and PARP Ex. 6.1.6 built most of it at PARP Ex. 6.1.6 home. However, PARP Ex. 6.1.6 did not have the tools or space to complete the supports, edging, or the "biscuiting."[10] So PARP Ex. 6.1.6 had one of PARP Ex. 6.1.6 help PARP Ex. 6.1.6 complete this work at the PARP Ex. 6.1.6 stated they completed all of this work during a single lunch hour.

The investigation also revealed the PARP Ex. 6.1.6 maintain in-house stock through surplus purchases on PARP Ex. 6.1.6 Purchase Card. The PARP Ex. 6.1.6 all agreed this was done in an effort to limit the amount of time they felt was wasted traveling to stores to continually purchase commonly used items. These surplus items are not purchased in separate transactions, and are assigned to the same PARP Ex. 6.1.6 work order number as the original project.

[9] See Exhibit 6.

[10] A carpentry technique used to join two pieces of wood together, whereby small holes are cut in the opposite edges of two pieces of wood, and the pieces are clamped together with glue.

[redacted] False Statements to OIG

OIG interviewed [redacted] at the initial stages of the investigation. During [redacted] interview, [redacted] provided multiple false and misleading statements to OIG Special Agents regarding the use and control of [redacted] Purchase Card, as well as the inventory oversight [redacted] provides. These false statements include, but were not limited to the following:

1. [redacted] *stated* [redacted] *was the only person who used* [redacted] *Purchase Card, and the only person who signed the receipts for these purchases.*
    - It is clear through an analysis of the signatures on the receipts, as well as every other witness interviewed by OIG, that [redacted] frequently provided [redacted] Purchase Card to [redacted] subordinates and directed them to utilize the Card. As [redacted] signed [redacted] monthly expense reports verifying all of the purchases made on [redacted] Purchase Card, [redacted] could not have been unaware of [redacted] employees' use of [redacted] Card.

2. [redacted] *stated* [redacted] *directs* [redacted] *assigned* PARP Ex. 6.1.6 *to write what supplies, if any, are needed to complete the project on the* [redacted] *work order ticket. This list is returned to* [redacted] *for* [redacted] *to procure the needed items.* [redacted] *stated* [redacted] *maintained these* PARP Ex. 6.1.6 *tickets for a period of* PARP Ex. 6.1.6.
    - OIG asked [redacted] to provide the PARP Ex. 6.1.6 tickets that related to the Purchase Card transactions since PARP Ex. 6.1.6 2016.[11] [redacted] provided approximately [redacted] work order tickets, which were in no discernable order. OIG reviewed all [redacted] documents to compare them to the Purchase Card receipts. Of these work order tickets, only [redacted] related to Purchase Card transactions. None of the tickets contained PARP Ex. 6.1.6 purported list of supplies to be purchased.

3. *In response to an OIG query of how* [redacted] *monitors inventory,* [redacted] *stated* [redacted] *was "pretty shrewd," and* [redacted] *will "keep an eye" on how much inventory* [redacted] *purchased that month, and how much should have been used based on the* PARP Ex. 6.1.6 *work order tickets.* [redacted] *will compare this to how much inventory* [redacted] *observes in their in-house inventory, and* [redacted] *will "start to ask questions" if* [redacted] *notices a discrepancy.*
    - [redacted] failed to maintain the work order tickets for 64% of [redacted] Purchase Card transactions, and another 36% did not contain any detailed information about the items purchased. Therefore, it would have been impossible for [redacted] to use the work order tickets as a means of inventory control. Additionally, all other witnesses interviewed by OIG stated there was no inventory control as multiple employees from other divisions utilized the PARP Ex. 6.1.6 supplies.

4. [redacted] *stated* [redacted] *visits* PARP Ex. 6.1.6 *at the project location to verify the status of work completed, approximately* [redacted] *of the time in order to provide quality*

[11] At the time the time of this request, [redacted] had made [redacted] purchases.

assurance that the PARP Ex. 6.1.6 *are accurately reporting the damage and necessary remediation. Additionally,* [redacted] *indicated* [redacted] *will go out to a location if the* PARP Ex. 6.1.6 *request "sends a red flag." As an example,* PARP Ex. 6.1.6 *stated* [redacted] *would be suspicious if a* PARP Ex. 6.1.6 *requested 10* PARP Ex. 6.1.6[12] *for one (1) location.*

- None of the witnesses interviewed could corroborate PARP Ex. 6.1.6 assertion of quality assurance. All of the witnesses interviewed indicated there was no review or quality assurance for their work. Further, it is clear that the purchase of surplus supplies was not a "red flag" for PARP Ex. 6.1.6, as it was common practice among the PARP Ex. 6.1.6.

5. PARP Ex. 6.1.6 *stated* [redacted] *used a generic work order number when* [redacted] *purchased replacements for* PARP Ex. 6.1.6. *He stated* [redacted] *Expense Report would always include who the replacement* [redacted] *was for.*
   - PARP Ex. 6.1.6 spent PARP Ex. 6.1.6 on PARP Ex. 6.1.6 transactions).[13] Of these [redacted] transactions, [redacted] did not include the name of the employee for whom the [redacted] was purportedly purchased.

Further, subsequent to OIG's interview where PARP Ex. 6.1.6 was questioned about [redacted] generic work order number [redacted] changed [redacted] use of this ticket. PARP Ex. 6.1.6 was interviewed on PARP Ex. 6.1.6, 2017. At that point, PARP Ex. 6.1.6 averaged [redacted] purchases per month assigned to the PARP Ex. 6.1.6. Subsequent to the interview, this number dropped to [redacted] total purchases for the next two months. However, it is clear [redacted] did not stop justifying Purchase Card transactions with generic work order numbers. In addition to the [redacted] transactions associated with the generic Work Order ticket PARP Ex. 6.1.6 completed [redacted] transactions which [redacted] ascribed to [redacted] different generic PARP Ex. 6.1.6 created in PARP Ex. 6.1.6. In one instance, PARP Ex. 6.1.6 created the generic work order ticket around the time PARP Ex. 6.1.6 was due, but [redacted] days after the initial purchase [redacted] ascribed to the ticket.

Relevant Statutes, Regulations, and Other Standards

Policy/Instruction 13.4/2 – Office of Inspector General, Section 4.02(d) Metro Employee Responsibilities

Policy/Instruction 18.11/1 – Purchase Card Policy

Asset Management Manual

OIG Investigative Findings

[redacted] lied to OIG Special Agents and deliberately provided misleading information that hindered the investigation. In spite of this, OIG was able to determine PARP Ex. 6.1.6 failed to comply with the Purchase Card Policies. PARP Ex. 6.1.6 routinely directed PARP Ex. 6.1.6 to take

[12] PARP Ex. 6.1.6

[13] See Exhibit 7.

PARP E Purchase Card for use at multiple stores. While PARP Ex 6.1.6 maintained receipts for these transactions, it is clear there was little to no oversight to ensure the purchased items were limited to what was necessary. While a superficial review of PARP Ex. 6.1.6 list PARP Ex 6.1.6 work orders as justification for the majority of his purchases, there were PARP E instances where the PARP Ex. 6.1.6 work order number was either invalid or clearly did not justify the purchases made. Further, there were PARP Ex 6 instances where the PARP Ex 6.1.6 work order number listed to justify the purchase was a generic work order created by PARP Ex. 6.1.6. These instances totaled PARP Ex 6.1.6.

Further, the statements from multiple witnesses, along with the photograph presented to OIG, make it clear that the inventory housed at the PARP Ex. 6.1.6 is not properly controlled or documented. This lack of controls has resulted in a widespread abuse of the inventory. Not only are the PARP Ex. 6.1.6 allowed to complete off the books projects utilizing WMATA property during WMATA business hours, these projects are often completed at the direction of PARP Ex 6.1.6. Further, the witnesses indicated many WMATA employees outside of PARP Ex. 6.1.6 unit are aware of the lack of inventory controls, and also engage in the undocumented use of these supplies.

This case was not presented for prosecution because of poor record keeping and inventory controls by PARP Ex 6.1.6. Therefore WMATA management should take whatever disciplinary action it deems appropriate with respect to PARP Er actions.

The investigation also revealed the WMATA storeroom system failed to meet the needs of the PARP Ex 6.1.6 division. This appears to be due to a combination of lack of training on the system with the appropriate PARP Ex 6.1.6 staff, and a lack of communication to ensure the Storerooms maintain the appropriate levels of stock items needed by PARP Ex 6.1.6. The BPAs that are in place are not properly utilized. Further, the dearth of any definite contracts in place for the PARP Ex 6.1.6 division prevent WMATA from receiving the savings benefits that could be achieved through the competitive bidding process.

Exhibits

1. Chart of purchases made despite BPA in place
2. BPA for PARP Ex 6.1.6 supplies
3. Chart of purchases made without a valid work order number
4. Chart of purchases that could not be justified based on the records
5. Chart of generic PARP Ex 6.1.6 ticket purchases
6. Photograph of "off the books" project
7. Chart of PARP Ex. 6.1.6 purchases

PARP Ex. 6.1.6
Kathryn Holpuch, Special Agent

PARP Ex. 6.1.6
Isabel Mercedes Cumming, AIGI

M E M O R A N D U M

SUBJECT: Management Assistance Report PARP Ex. 6.1.6 DATE: August 16, 2017

FROM: OIG – Geoffrey Cherrington

TO: GMGR – Paul J. Wiedefeld

RE: Purchase Card Misuse ROI #17 0021-I

The Office of Inspector General is forwarding this memorandum to you, which identifies several conditions within the PARP Ex. 6.1.6 division at the PARP Ex. 6.1.6 that facilitate conditions where fraud, waste, and abuse are occurring. Please take the appropriate actions to correct these conditions.

1. Construction related inventory housed at the PARP Ex. 6.1.6 is not properly controlled or documented. Only the smaller inventory items, such as PARP Ex. 6.1.6, are housed in a locked storeroom. The rest of the inventory, to include PARP Ex. 6.1.6, etc., are stored on the PARP Ex. 6.1.6. None of the inventory is tracked or logged as it enters or leaves the PARP Ex. 6.1.6. This creates an environment where PARP Ex. 6.1.6 employees could easily remove items without detection. Because of the lack of controls, it is also possible for employees outside of PARP Ex. 6.1.6 to also engage in the undocumented use of these supplies.

2. The majority of commonly used supplies such as PARP Ex. 6.1.6 are purchased at the maximum retail price through individual purchase cards. PARP Ex. 6.1.6 does not have any contracts in place for the purchase of these items.

3. While there are three Blanket Purchase Agreements in place to purchase PARP Ex. 6.1.6 employees are still using purchase cards to procure these materials. OIG's investigation also found a lack of training and understanding of the proper use of storeroom procedures by PARP Ex. 6.1.6 personnel.

Please respond in writing or have a member of your staff respond by September 18, 2017, to Assistant Inspector General for Investigations, Isabel Cumming, regarding the corrective actions taken or planned as a result of this investigation. Also, please provide estimated dates and/or timelines for implementing these corrective actions.

Attachment

cc: COO – J. Leader
INCP – E. Christensen
COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Assistance Report DATE: October 26, 2017

FROM: OIG – Geoffrey Cherrington PARP Ex. 6.1.6

TO: GMGR – Paul J. Wiedefeld

RE: PARP Ex. 6.1.4 Procurement
OIG Case No. 17-0024-I

The Office of Inspector General (OIG) received an allegation that the PARP Ex. 6.1.6 provided exceedingly stringent specifications for the procurement of PARP Ex. 6.1.4 to favor the PARP Ex. 6.1.6 OIG identified systemic problems within the PARP Ex. 6.1.6 in the procurement of PARP Ex. 6.1.4. OIG is forwarding this memorandum to assist in taking the appropriate actions to correct these conditions.

1. PARP Ex. 6.1.4 supplied by PARP Ex. 6.1.6 is not compliant with the contract specifications. Specifically, it does not contain sufficient treatment to prevent PARP Ex. 6.1.4. Independent testing of PARP Ex. 6.1.4 samples confirmed the presence of PARP Ex. 6.1.4. Although PARP Ex. 6.1.6 provided certification of PARP Ex. 6.1.4, their testing laboratory used a test standard to merely identify the presence of an PARP Ex. 6.1.4 rather than test the PARP Ex. 6.1.4 for its susceptibly for PARP Ex. 6.1.4. PARP Ex. 6.1.6 should require all future testing of PARP Ex. 6.1.4 to be compliant with current standards. OIG's laboratory test results are included with this memorandum for reference.

2. PARP Ex. 6.1.6 personnel indicated a preference for PARP Ex. 6.1.4 due to its PARP Ex. 6.1.4. However, PARP Ex. 6.1 is also the most expensive PARP Ex. 6.1.4. PARP Ex. 6.1.6 personnel acknowledged the lack of consideration of other PARP Ex. 6.1.4 such as PARP Ex. 6.1.4. PARP Ex. 6.1.6 should investigate options for other less expensive PARP Ex. 6.1.4 materials for future purchases.

3. PARP Ex. 6.1.6 did not provide an independent test certification for the PARP Ex. 6.1.4. PARP Ex. 6.1.6 used a laboratory that has close ties to another company that provided the vendor with a line of credit to procure the PARP Ex. 6.1.4. This created an organizational conflict of interest. PARP Ex. 6.1.6 should require future laboratory testing companies to provide certification that they do not have any business or personal relationships with the PARP Ex. 6.1.4 vendor.

Please respond in writing by November 27, 2017 to Assistant Inspector General for Investigations, Isabel Cumming, regarding the corrective actions taken or planned as a result of this investigation. Provide estimated dates and/or timelines for implementing these corrective actions.

Attachment

cc: COO – J. Leader
INCP – E. Christensen
COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Alert

DATE: December 21, 2017

FROM: OIG – Geoffrey Cherrington PARP Ex. 6.1.6

TO: GMGR – Paul J. Wiedefeld

RE: Terminated employee, PARP Ex. 6.1.6
OIG Case No PARP Ex. 6.1.6

The Office of Inspector General (OIG) is transmitting this Management Alert to you to elevate significant concerns about the hiring of a contractor within PARP Ex. 6.1.6

On PARP Ex. 6.1.6, 2017, the OIG learned PARP Ex. 6.1.6 was scheduled to attend a one day PARP Ex. 6.1.6 training session to be held at the Jackson Graham Building (JGB) on PARP Ex. 6.1.6 2017. Training documentation obtained by the OIG indicated PARP Ex. 6.1.6 had been hired as a contractor by PARP Ex. 6.1.6 of PARP Ex. 6.1.6. Contractor training is conducted by WMATA's Department of Safety and Environmental Management (SAFE).

PARP Ex. 6.1.6 was terminated from employment with the Washington Metropolitan Area Transit Authority (WMATA) for PARP Ex. 6.1.6 as a result of information developed during an OIG overtime abuse investigation. The termination was based primarily on PARP Ex. 6.1.6

At the time of termination, PARP Ex. 6.1.6 was employed as a . OIG confirmed through Labor Relations (LABR) that PARP Ex. 6.1.6

The requirements for contractors involved in PARP Ex. 6.1.4 are specified in Request for Proposals (RFP) No. PARP Ex. 6.1.4 Among other things, the RFP specifies that contractor personnel must complete the requisite safety training and obtain a vendors' badge. Pursuant to WMATA Policy/Instruction 6.10/5, approved 5/18/2011, contractor employees and candidates for employment must also undergo and pass a criminal background screening before being eligible to work on WMATA property and facilities.

On PARP Ex. 6.1.6 2017, OIG confirmed that PARP Ex. 6.1.6 attended and successfully completed the [redacted] training, and [redacted] has been issued the requisite approval documentation and vendors' badge. This will allow [redacted] general access to otherwise restricted areas generally referred to as PARP Ex. 6.1.1 OIG learned PARP Ex. 6.1.6 began working on PARP Ex. 6.1.6 as a contractor on behalf of PARP Ex. 6.1.6 [redacted] on PARP Ex. 6.1.6 2017.

According to Section 22 of the RFP, the Office of Procurement and Materials (PRMT) contracting officer has the authority to determine if a contractor's employee is either "unsuitable" to perform work on the project, or whose participation "is deemed to be contrary to the best interests of the Authority." On PARP Ex. 6.1.6, 2017, OIG contacted the contracting officer in this matter who indicated it would be counter to WMATA's best interests to allow PARP Ex. 6.1.6 to perform work for WMATA while PARP Ex. 6.1.6 [redacted] The Department of Human Resources and LABR were also consulted on this matter, and they concurred that the authority granted to the contract manager within the language of the RFP provides sufficient discretion to prohibit PARP Ex. 6.1.6 from engaging in work as a contractor within WMATA facilities and property.

cc: COO – J. Leader
IBOP – J. Kuo
INCP – E. Christensen
COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Alert Report DATE: January 4, 2018

FROM: OIG – Geoffrey Cherrington PARP Ex. 6.1.6

TO: GMGR – Paul J. Wiedefeld

RE: Online Fraud Targeting WMATA
OIG Case Number 17-0116-C

The Office of Inspector General (OIG) is transmitting this Management Alert to update you on the recent targeted attempt to use fraudulent email correspondence to induce a Washington Metropolitan Area Transit Authority (WMATA) employee to wire transfer funds.

For the past sixteen months, the OIG has been tracking various attempts at online and wire fraud, commonly referred to as phishing, spear-phishing, or purchase order fraud, targeting WMATA. This information has been shared with the Federal Bureau of Investigation (FBI), which has provided the OIG with assistance and support in identifying and shutting down these cyber-crime entities. According to the information developed thus far, most, if not all, of these incidents have been coordinated by international group(s) based in Nigeria.

Typically, the individuals involved have establish fraudulent domain names and email accounts which are very similar to what one might reasonably believe to be an actual WMATA email correspondence. Recent examples of the so-called "account spoofing techniques" used against WMATA include: PARP Ex. 6.1.5 [redacted] The emails are directed to individuals both internal and external to WMATA, usually claiming to be a senior-level WMATA employee. The individuals either seek to purchase equipment from an outside vendor, or receive payment for equipment or services to be made from within WMATA.

The most recent of these online attacks occurred via a series of emails ending on PARP Ex. 6.1.6 [redacted], 2018. An individual purporting to be PARP Ex. 6.1.6 [redacted] attempted to persuade a PARP Ex. 6.1.6 [redacted] to wire transfer PARP Ex. 6.1.6 to the bank account of an entity supposedly entitled to a payment by WMATA for some unspecified service. A follow-up email made a second attempt, reducing the amount to PARP Ex. 6.1.6. As with other such attempts, the ruse failed, but it is worth noting this attempt was somewhat less sophisticated than what has been seen in previous incidents.

Through investigation and analysis, OIG has determined the originating email claiming to be from PARP Ex. 6.1.6 was actually a compromised PARP Ex. 6.1.6 account. When the WMATA

recipient noticed the email was not connected to a WMATA account, [redacted] became suspicious and made further internal inquiries; consequently, the scheme was defeated and no money was ever exchanged. The associated email and bank account information has been sent to the FBI for further analysis and tracking. The Metro Transit Police Department (MTPD) has been apprised of the situation and provided with the result of the OIG analysis. Based on what is known thus far, it is highly likely that this fraud attempt, as in the case of the previous incidents, was coordinated by actors operating out of Nigeria.

As in previous cases, it appears the subjects involved are using details found online and specifically the WMATA website to gather information on WMATA departments, staffing, email addresses, and billing information. The attackers then disguise themselves as actual WMATA personnel with malicious intent, targeting individuals both internal and external to WMATA. In cases where WMATA employee identities have been used to facilitate a fraud attempt, the OIG has advised respective personnel of the situation. In all of the cases seen to date, the goal has been to convince a vendor to ship equipment to what is believed to be a WMATA facility, or convince a WMATA employee to submit payment under the false assumption that a legitimate service has been provided.

The following is a list of recommendations which may assist in limiting WMATA's exposure to online fraud, the compromise of sensitive data, and targeted cyber-attacks. This information is provided for your review and does not require a response:

- Employees should be reminded to remain diligent in reviewing the source of emails which are unusual in nature or are seeking approval for the transfer of material or funds. Simply put, always use logic before opening any email.
- Where possible, limit organizational chart and email contact information posted on the WMATA website.
- Consider posting a notice on the WMATA website warning of phishing and purchase order scams, along with a telephone number for vendors to confirm the authenticity of an order. Many universities in the United States have done this and have seen a reduction in incidents; FBI subject matter experts also believe it is a useful tool.
- Ensure spam and phishing filters are up to date.
- Provide ongoing notifications to WMATA employees regarding the latest schemes. Based on conversations the OIG has had with WMATA employees relating to cyber-fraud attempts, it is clear that many employees are completely unaware of how this type of fraud occurs. Simply advising employees on how to spot basic indicators such as misspellings, odd vocabulary, or conflicting URL information can be highly effective in combating this problem.
- Ensure employees understand the nature of this threat. As in the case of this most recent incident, phishing has become more sophisticated than a suspicious email tempting a random individual to click on a link. Cyber-criminals are now targeting specific individuals within the WMATA organization.

M E M O R A N D U M

SUBJECT:	Management Alert [redacted]	DATE: March 28, 2018
FROM:	OIG – Geoffrey A. Cherringto[redacted]	
TO:	GMGR – Paul J. Wiedefeld	

RE: Internal Controls for Surplus/Obsolete and Unclaimed Lost & Found Property
OIG Case No. 17-0023-I

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate significant concerns about the sale of surplus/obsolete WMATA property.

An OIG investigation has been initiated after an anonymous allegation was received alleging that an [redacted] with [redacted], was rigging bids for sales in exchange for cash and other items. OIG conducted an investigation into similar allegations in 2014.[1] That joint investigation between Metro Transit Police Department (MTPD) and the OIG resulted in a criminal conviction of the Subject, as well as termination from WMATA. As a result of that investigation, internal controls were adopted to prevent future theft. However, these controls focused on incoming inventory for surplus/obsolete property, and did not adequately cover the sale of this property.

During the current investigation, OIG was not able to substantiate the allegations due to a lack of internal controls. While there was proper documentation for stock and barcoded items, this documentation did not extend to non-stock items without a barcode.[2] This category of property includes WMATA [redacted]. OIG discovered these were shipped in bulk to [redacted] without any inventory logs.[3] While the [redacted] maintain a handwritten log of property received at [redacted], there is no way to verify whether their log contains accurate information.

[1] See OIG case 14-0019-I.

[2] While [redacted] SOP [redacted] requires all WMATA assets without a barcode be recorded within the transfer package with serial or item number, description, transfer date and quantity. OIG observed this procedure was not followed.

[3] Since the OIG brought this to the attention of the [redacted] has informed OIG that [redacted] has started to keep an unofficial inventory log of all the [redacted] shipped to [redacted] for sale.

Unclaimed property from Lost & Found is also sent to PARP Ex. 6.1.1 for sale. These items are accompanied by itemized lists from Lost & Found, although the list contains only general descriptions and not serial numbers. OIG learned there is no coordination between Lost & Found and MTPD to ensure the unclaimed property, such as PARP Ex. 6.1.1 or other serialized property, has not been reported stolen. This could result in a scenario where WMATA could be selling stolen property, in violation of Maryland Criminal Code 7-104(c).

The items from Lost & Found, as well as WMATA PARP Ex. 6.1.1 are sold "in bulk."[4] There is no paper trail to ensure the bulk sales include all of the items received by PARP Ex. 6.1.1. As an example, Lost & Found may have sent 100 PARP Ex. 6.1.1 to PARP Ex. 6.1.1. The description on the sales paperwork for these PARP Ex. 6.1.1 would only list PARP Ex. 6.1.1 without any quantity or further description. There is no documentation or safeguards in place to prevent someone from removing any number of these PARP Ex. 6.1.1 from the PARP Ex. 6.1.1 and converting them to a private sale.

PARP Ex. 6.1.1

As noted, this information was developed pursuant to an OIG investigation. Although none of the allegations were substantiated, due to the seriousness of the potential management consequences, this information is being forwarded without delay.

cc: COO – J. Leader
IBOP – J. Kuo
INCP – E. Christensen
COUN – P. Lee

[4] In accordance with PARP Ex. SOP PARP Ex. 3.1.5.
[5] OIG was told by PARP Ex. personnel that they purchased the cameras after their request for cameras was denied by MTPD due to lack of funding.

M E M O R A N D U M

SUBJECT: Management Alert DATE: April 25, 2018

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

RE: Fraudulent Withholding Exemption
OIG Case No. 18-0316-C

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate significant concerns about unusual and possibly illegal activity by Washington Metropolitan Area Transit Authority (WMATA) employees regarding exemptions claimed on their Form W-4 tax withholdings.

During the course of an unrelated investigation, OIG discovered that more than 1,400 WMATA employees are currently claiming 99 exemptions for their tax withholding. This results in a situation where those employees are, in effect, not paying any federal or state income taxes. Numerous employees have claimed 99 exemptions for several years.

WMATA employees can easily change their withholding exemptions through PeopleSoft via the Self-Service option. No review or approval is required for these changes. The employee is required, however, to certify under penalties of perjury that they are entitled to the number of exemptions entered on the electronic form.

According to the Federal Tax Statute, Title 26, United States Code 7205(a) Withholding On Wages – "Any individual required to supply information to his employer {in this case WMATA} under section 3402 who willfully supplies false or fraudulent information…, in addition to any other penalty provided by law, upon conviction thereof, be fined not more than $1000 and imprisoned not more than one year, or both." Employees who attempt to thwart the income tax wage withholding system by submitting false W-4 information to their employers are in violation of this statute.

Although a violation of Section 7205(a) is a misdemeanor, since WMATA has a substantial number of employees involved, the OIG and IRS could refer these cases for felony prosecutions for filing a false or fraudulent Form W-4 as an affirmative act in what is known as a Spies-evasion (tax evasion section 7201) charge.

The only exception to the exemption withholding is if the employee certifies that they are claiming exempt status. In order to claim this status they must meet two conditions:

- In the prior year they had a full refund of their federal income tax because they had no tax liability and,
- In the current year they expect to have a full refund of all federal income tax withheld because they expect to have no tax liability.

WMATA is not required to deduct and withhold any tax upon wages if an employee certifies that he/she meets the exceptions cited above.

OIG and tax officials are conducting a joint investigation and have not yet determined if the WMATA employees claiming 99 exemptions meet these exceptions. This information is being provided to you in advance of the completion of our investigation for any action you deem necessary as this could have a negative impact on the affected employees, and a potential negative impact on WMATA given the large number of employees engaged in this practice.

cc: IBOP – J. Kuo
INCP – E. Christensen
COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Alert

DATE: November 16, 2018

FROM: OIG – Geoffrey A. Cherrington PARP Ex. 6.1.6

TO: GMGR – Paul J. Wiedefeld

RE: Alleged Inappropriate Behavior
OIG Case No. PARP Ex. 6.1.6

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding a complaint alleging inappropriate behavior on the part of the Washington Metropolitan Area Transit Authority (WMATA) PARP Ex. 6.1.6, at a PARP Ex. 6.1.6.

On PARP Ex. 6.1.6 2018, the OIG received an email from the PARP Ex. 6.1.6 advising of a complaint they had received via their online "Contact Us" portal. The complaint, which included two short video clips allegedly documenting the event, described an incident which occurred at PARP Ex. 6.1.6 on WMATA property involving PARP Ex. 6.1.6 and an unidentified, PARP Ex. 6.1.6.

The video appears to show PARP Ex. 6.1.6. At one point, PARP Ex. 6.1.6

In the complainant's email to PARP Ex. 6.1.6 behavior is described as PARP Ex. 6.1.6 as well as PARP Ex. 6.1.6 claiming PARP Ex. 6.1.6 The complainant refers to the video clips as PARP Ex. 6.1.6
In both the email to the PARP Ex. 6.1.6 and in follow-up emails with OIG, the complainant claims to have PARP Ex. 6.1.6

This complaint is being forwarded to you for any action you deem necessary. The OIG does not intend to investigate the matter further at this time.

cc: COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Assistance Report DATE: February 5, 2019

FROM: OIG – Geoffrey A. Cherrington [redacted]

TO: GMGR – Paul J. Wiedefeld

RE: Employee Identification Cards
OIG Case No. 19-0002-I

The Office of Inspector General (OIG) has identified a common practice throughout the Washington Metropolitan Area Transit Authority (WMATA) involving the duplication and misuse of identification badges (IDs). OIG began investigating this issue after receiving notification from the Metro Transit Police Department (MTPD) about the recovery of 15 duplicated IDs from a wide range of employees, including [redacted] between [redacted] 2018 and [redacted] 2019. OIG received anecdotal information that the practice is much more widespread throughout WMATA.

The OIG's investigation focused on the reasons for the extensive duplication of WMATA identification badges and how the duplicate IDs were used throughout WMATA.[1] OIG found evidence that employees used the duplicate IDs for a range of reasons, from simple convenience to outright fraud.

The most concerning of the reasons given, was that employees were using duplicate IDs to fraudulently clock each other into the Kronos[2] time keeping system.[3] The OIG verified that employees would work in groups to exchange their duplicate IDs, thus creating a network of individuals they could rely on to clock them in or out of work, when for example, the employee was late for work. The OIG was unable to substantiate how many employees participated in this scheme. However, OIG determined WMATA employees worked in various fields and departments. OIG is preparing a final Report of Investigation, which will include the identities of the involved employees.

[1]Metro's Policy Instruction Manual (PI) is void of any policy instructing employees not to make copies of their WMATA ID badges. The back of most IDs state "It is NOT transferable" and there is no further instruction.

[2]WMATA suspended Kronos in the summer of 2018.

[3]The Kronos system appears to need only a barcode on the IDs to enter an employees' time and therefore, a paper copy was sufficient.

The OIG found that the majority of the employees were using the duplicate IDs out of convenience.[4] Employees repeatedly stated that they were fearful of leaving their actual IDs at home or in another vehicle and would not be able to enter WMATA facilities. The OIG concluded that the duplication of WMATA ID badges is not isolated to one department, and may be a common practice throughout the authority.

Throughout the OIG investigation, employees repeatedly stated that Special Police Officers (SPOs) never closely checked their badges and all they had to do was simply flash the duplicate copy of their ID to gain access to the secured locations. Consequently, the OIG conducted surveillance at six WMATA secured locations; namely New Carrollton Bus Division, New Carrollton Rail Yard, Carmen Turner Facility, Bladensburg Bus Division, Greenbelt Rail Yard, and Montgomery Bus Division, to determine if SPOs were checking drivers and passengers for WMATA ID badges.

The OIG found a wide range of activity by the SPOs. SPOs at the PARP Ex. 6.1.6 Bus Divisions were thorough and checked OIG Special Agents' badges upon entry. In contrast, SPOs failed to check OIG Special Agents' badges at [redacted] There were no SPOs at the security booths located at the entrances of the PARP Ex. 6.1.6 .[5]

The OIG's investigation raises great concern over the security of WMATA's facilities. If an unauthorized individual involved in criminal or terrorist activity used a duplicated ID, WMATA's transportation infrastructure and the Nation's capital would be exposed to potentially devastating consequences.

OIG forwards this memorandum to assist management to take appropriate action and makes the following recommendations:

1. Update WMATA's Policy Instruction Manual (P/I), to prohibit the duplication of WMATA IDs. Proposed language follows:

   "Employees are not permitted to make, duplicate, possess, or use imitation of any and all WMATA issued cards, including but not limited to, Employee Identification Badges, Parking Permits, Metro decals, Blue Tag cards, and Personnel Accountability Tags."

2. Distribute an authority wide communication to all employees notifying them of the new policy change. Instruct all employees with any copies of their WMATA issued cards to destroy them, or turn them in to an SPO immediately for destruction. The communication should detail the consequences if employees are found in possession or attempting to utilize duplicates of their WMATA issued identification cards after that date.

---

[4]The contractor used a fake ID along with PARP Ex. 6.1.6 . The contractor stated that at any moment someone could demand to see whether [redacted] had [redacted] training. [redacted] was concerned that [redacted] might leave [redacted] actual ID in [redacted] truck so [redacted] made a copy.
[5]OIG Agents observed several vehicles enter the unsecured properties, gaining access to trains and the roadway.

3. If WMATA reinstates Kronos, investigate whether the manufacturer can make modifications to the time keeping system, to ensure that employees can no longer use duplicated WMATA ID badges for time entry.

4. Ensure SPOs are stationed at all secured WMATA facility access points.

5. Conduct additional training of SPOs regarding physical inspections procedures of WMATA ID badges for all employees/contractors entering a secured facility.

Please respond in writing by February 15, 2019 to Deputy Inspector General for Investigations, Kimberly Howell, regarding the actions taken or planned because of this investigation.

cc: COUN – P. Lee
INCP – E. Christensen
COO – J. Leader

M E M O R A N D U M

SUBJECT: Management Alert PARP Ex. 6.1.6 DATE: March 12, 2019

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

RE: Safety Concerns
OIG Case No. 19-0072-C

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding a potential safety issue involving the purchase of unapproved bus PARP Ex. 6.1.4 for WMATA buses. During the course of an unrelated investigation, OIG learned that WMATA sought bids for the procurement of PARP Ex. 6.1.4 for use on its bus fleet.[1] PARP Ex. 6.1.4 responded to the solicitation by bidding on one of the specific part numbers PARP Ex. 6.1.4 and included what was subsequently determined to be the name of a manufacturer PARP Ex. 6.1.4 On PARP Ex. 6.1.6 2018, PARP Ex. 6.1.4 was awarded Purchase PARP Ex. 6.1.4 to supply WMATA with PARP Ex. 6.1.4 at a total cost of PARP Ex. 6.1.4.

PARP Ex. 6.1.4 delivered PARP Ex. 6.1.4 on PARP Ex. 6.1.6, 2018, and the remaining PARP Ex. on PARP Ex. 6.1.6 2018.[2] The PARP Ex. 6.1.4 had an approved part number PARP Ex. 6.1.4 listed on labels reportedly affixed to the outside of the boxes.[3] WMATA staff was apparently unaware at the time of the aforementioned deliveries that the PARP Ex. 6.1.4 were not approved for use on WMATA buses and mistakenly relied on the misleading labels containing the approved part number. PARP Ex. 6.1.6 advised OIG that WMATA first learned of the improper product substitution as a result of a phone call the Office of Bus Maintenance (BMNT) received from PARP Ex. 6.1.4 requesting feedback on these PARP Ex. 6.1.4.[4] BMNT reportedly informed PARP Ex. 6.1.4 that WMATA did not use the PARP Ex. 6.1.4. PARP Ex. 6.1.4 then reportedly indicated that they sold these PARP Ex. 6.1.4 to PARP Ex. 6.1.4. Independent of this phone call and WMATA's realization that PARP Ex. 6.1.4 substituted PARP Ex. 6.1.4,

[1] The solicitation included specific approved vendor part numbers.
[2] According to the packing slip that accompanied the PARP Ex. 6.1.6 2018 delivery, the remaining PARP Ex. 6.1.4 were backordered.
[3] It was not known at the time that this approved PARP Ex. 6.1.5 was improperly associated with this product PARP Ex. 6.1.4.
[4] PARP Ex. 6.1.6 advised OIG that PARP was unaware of any call that PARP office received from PARP Ex. 6.1.4 requesting feedback on PARP Ex. 6.1.4. Rather, PARP Ex. 6.1.6 claimed that PARP first learned of the issue with PARP Ex. 6.1.4 from a PARP Ex. 6.1.6 2018 email from the Four Mile Division reporting problems with PARP Ex. 6.1.4.

at least 11 buses reportedly experienced PARP Ex. 6.1.4, some within days of installation of these [redacted].[5]

OIG's review of the available documentation revealed that PARP Ex. 6.1.4 were initially quarantined in PARP Ex. 6.1.6 2018. The documentation further indic[redacted]TA returned [redacted] to PARP Ex. 6.1.4 and received a credit for these returned parts on PARP Ex. 6.1.6, 2019. PARP Ex. 6.1.6 2018 email to PARP Ex. 6.1.6, which copied PARP Ex. 6.1.6, indicated that "BMNT had to recall all the buses with these PARP Ex. 6.1.4 to remove them and replace them with approved PARP Ex. 6.1.4 that we had in stock." However, PARP Ex. 6.1.6 subsequently advised OIG that these PARP Ex. 6.1.4 were still on WMATA buses and that [redacted] email in this regard was inaccurate. PARP Ex. 6.1.6 confirmed that only PARP Ex. 6.1.4 were returned to PARP Ex. 6.1.4.

Since the PARP Ex. 6.1.4 are not approved for use on WMATA buses and have reportedly experienced PARP Ex. 6.1.4 on at least 11 buses, OIG attempted to determine the status of the remaining PARP Ex. 6.1.4 that have not been returned to PARP Ex. 6.1.4. OIG contacted PARP Ex. 6.1.6 on PARP Ex. 6.1.6, 2019, to determine whether any of the PARP Ex. 6.1.4 supplied by PARP Ex. 6.1.6 were still installed on WMATA buses.[6] PARP Ex. 6.1.6 initially indicated that [redacted] could not provide OIG with an answer. PARP Ex. 6.1.6 further stated that [redacted] staff would have to research the PARP Ex. 6.1.4 system to determine which buses these PARP Ex. 6.1.4 were installed on and whether these [redacted] were ever removed.[7] PARP Ex. 6.1.6 contacted OIG on [redacted] 2019, and indicated that it was impossible to determine which buses had the PARP Ex. 6.1.4 [redacted] installed. [redacted] opined that the PARP Ex. 6.1.4 did not present a safety concern and were just [redacted]. However, PARP Ex. 6.1.6 agreed that the PARP Ex. 6.1.4 are not approved for use on WMATA buses. OIG also spoke to PARP Ex. 6.1.6 [redacted] on PARP Ex. 6.1.6 2019, concerning the status of the PARP Ex. 6.1.4. [redacted] indicated that [redacted] was not familiar with the PARP Ex. 6.1.4 issue but would research the matter.[8] [redacted] subsequently sent an email to OIG indicating that only PARP Ex. 6.1.4 were received and [redacted] were backordered. [redacted] further indicated, "It is very difficult to determine as to which Bus Work Order these PARP Ex. 6.1.4 were issued/installed, since parts inventory in the Store Rooms is managed by WMATA Stock #s, and not by manufacturer/brand names. Buses repaired with these [redacted] were reported for PARP Ex. 6.1.4, within 3-4 days of repairs. Given that [redacted] related complaints/defects are addressed/repaired as a priority, it is highly unlikely that any bus with PARP Ex. 6.1.4 is still in service." OIG again spoke to [redacted] and advised [redacted] that WMATA records indicated that all PARP Ex. 6.1.4 were received. [redacted] later sent an email to OIG advising that PARP Ex. 6.1.6 will research the status of the PARP Ex. 6.1.4.

Although OIG will continue to investigate the circumstances surrounding PARP Ex. 6.1.4 product substitution of the PARP Ex. 6.1.4, this Management Alert is being provided so that immediate

[5] OIG has not yet been provided with documentation detailing what, if any, action was taken with respect to the [redacted] on these 11 buses.
[6] PARP Ex. 6.1.6 advised OIG that [redacted] was calling from the airport as [redacted] was in travel status at the time.
[7] PARP Ex. 6.1.6 2018 email to several staff members indicated that WMATA experienced similar problems with this PARP Ex. 6.1.4 vendor and had to disqualify them. Indeed, OIG obtained a PARP Ex. 6.1.6, 2016 Material Discrepancy Report, which noted the rejection of [redacted] PARP Ex. 6.1.4 by [redacted].
[8] It should be noted that [redacted] and [redacted] were included on several emails in PARP Ex. 6.1.6 2018 pertaining to this matter.

appropriate action can be taken to ensure the safety of the bus fleet with respect to the [redacted] that have not been returned to the vendor.

cc: COUN – P. Lee

M E M O R A N D U M

SUBJECT: Management Assistance Report
Complaint from Contractor
(OIG Complaint No.: 19-0249-C)

DATE: April 22, 2019

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) received a complaint from a "Contractor" alleging that Washington Metropolitan Area Transit Authority (WMATA) procurement staff were unresponsive to questions, making it difficult for the Contractor to bid for a project, i.e., Request for Proposals (RFP) for Task Orders 6 and 7 related to the Accounting IDIQ contract [redacted] for Financial Management and Audit Readiness Support Services.[1] A Contractor employee was also informed that they asked too many questions. In addition, the Contractor reported an incomplete website posting for RFP # [redacted]— the website subsequently posted an "amended" document, with its full RFP, once the OIG notified the procurement office of the omission on the website.

The OIG conducted a limited review of Contractor's complaint. The following information outlined in this memorandum is being provided to alert you to the results of our review.

OIG Investigative Findings

1. Complaint:

   OIG interviewed the Contractor's two senior-level employees (i.e., "Senior Manager" and "Partner") regarding the complaint. They provided relevant emails and documents for OIG's review. During the process of the Contractor's proposals for Task Orders 6 and 7, the Senior Manager primarily communicated with the assigned [redacted]

[1] The undisclosed contractor is one of six (6) vendors, having the base, Indefinite Quantity/Indefinite Delivery (IDIQ) contract award ([redacted] for subsequent task order solicitations.

[redacted], and two [redacted] and [redacted], via clm@wmata.com.[2]

According to the Senior Manager, areas of difficulty and confusion involved [redacted], [redacted] email and the incorrect CLM system data for the Contractor's point of contact (POC) for information. For example, on PARP Ex. 6.1.6, 2018, via email, the Senior Manager requested [redacted] to add the requestor's email address on his "event notification list" and anything related to PARP Ex. 6.1.4 for the Contractor because the employee did not receive [redacted] email directly. [redacted] then confirmed that [redacted] would do so; however, [redacted] did not send the Senior Manager any subsequent event notification related emails. Instead, [redacted] emails were forwarded by the Contractor's partner to the appropriate employee. The Contractor was the original recipient of the contract award notification.

During the interview, the OIG confirmed that [redacted] had sent no message stating the Contractor asked too many questions. The Senior Manager explained the possibility that the employee could have interpreted [redacted] email requesting only one POC, not multiple POCs, as [redacted] message that the Contractor asked too many questions.

Separately, on PARP Ex. 6.1.6, 2018, the Senior Manager sent an email to CLM stating that the contractor employee (employee) "cannot locate the events" to upload Task 6 and 7 proposals. The Senior Manager informed CLM that the employee is the Contractor's new POC and that [redacted] had not received any system generated emails for the task orders. CLM replied with a link to "User Guidance" and instruction for getting a new password for the Senior Manager. On PARP Ex. 6.1.6, 2018, the CLM team [redacted] informed the Senior Manager that the team is working on the "technical issues" and that the event is being extended. On that same date, [redacted] informed all parties that the proposal due date for Task 6 and 7 was being extended to April 3, 2018. The Contractor was able to submit its Task Order 6 and 7 proposals by uploading them via the website portal on PARP Ex. 6.1.6, 2018.

On PARP Ex. 6.1.6 2018, [redacted] requested all vendors to send their proposals by email—as requested, on that same date, the Senior Manager sent [redacted] both task proposals by email. On PARP Ex. 6.1.6 2018, [redacted] then sent an email to all vendors that [redacted] Task Order 6 had been awarded to [redacted].[3] Task Order 7 solicitation had been cancelled.

[2] Clm@wmata.com serves as a "tier one" POC for vendor's technical issues such as a password reset and the like. CLM is a concept for a comprehensive, end-to-end procurement process. It builds on existing systems such as certain PeopleSoft modules including Purchasing, Procurement Contracts, etc.

[3] The award was evaluated for the overall "best value" to WMATA.

On PARP Ex. 6.1.6, 2018, the Senior Manager learned that the Contractor's POC information had not been updated in the system. The employee again contacted CLM [redacted] via clm@wmata.com. On PARP Ex. 6.1.6, 2018, [redacted] confirmed update of the Contractor's POC information by sending the employee a screen shot of the updated email address.

Lastly, in another matter related to an OIG solicitation, the Contractor discussed a different matter as an "example" of problems with the solicitation process. Specifically, in PARP Ex. 6.1.6 2019, the Contractor noticed an incorrect RFP # [redacted] posting on WMATA's website. The solicitation posting was incomplete and only contained three words PARP Ex. 6.1.4 [redacted] on a single page for the RFP—there was no actual RFP posted on the website. The Contractor contacted WMATA's procurement staff regarding the problem but no one called them back. The website subsequently posted an "amended" document, with its full RFP, once the OIG informed the procurement office of the mistake. This process caused, among other things, caused a delay in the award of the contract.

2. Interview of WMATA Procurement Staff

   a. [redacted], of the WMATA CLM Team, was interviewed regarding his contact with the Senior Manager. On PARP Ex. 6.1.6, 2018, [redacted] responded to the Senior Manager's request for assistance (via clm@wamat.com) and eventually updated the employee's contact information. According to [redacted] in general, the CLM team serves as a "tier one" POC that addresses vendor's technical issues such as a password reset and the like. They do not have access to, nor do they provide support to specific contract event or contract business-related information. The previous CLM responder [redacted] who exchanged emails with the Senior Manager no longer works with WMATA; [redacted] believed [redacted] scope of work would have been as similar as his own, as [redacted] would not have provided any contract event or contract business-related support.

   b. [redacted], [redacted], was interviewed regarding the complaint at issue. During the interview, [redacted] reviewed the task order file and copies of emails that he had exchanged with the Senior Manager. Regarding the Contractor's POC issue, [redacted] explained that [redacted] does not have access to the system module that would allow [redacted] to update vendor's POC information. The Senior Manager was referred to contact CLM. In addition, [redacted] pointed to the RFP, Page 2, Notice to All Vendors, where it states that "it is the vendor's responsibility to register and update all information in WMATA Supplier Portal.

[redacted] acknowledged replying to the Senior Manager's email that [redacted] would add the employee to [redacted] own email list; however, [redacted] had forgotten to do it. Nevertheless, [redacted] reiterated that someone within the Contractor's office did continue to receive [redacted] subsequent emails regarding the task solicitation information. [redacted] explained that [redacted] had asked for a single POC, as communicating with multiple vendor POCs was difficult for [redacted]

[redacted] explained that vendors can only upload their proposals before due date in the system—all six vendors submitted their proposals before due date, [redacted] 2018.

[redacted] did not remember [redacted] reason for the [redacted] 2018 email requesting all proposals be sent to [redacted] via email; however, [redacted] explained that there are instances in which [redacted] would request to receive vendor proposals via email and sometimes even after past their due date in order to remedy technical system issues. In addition, [redacted] sends [redacted] emails to check whether or not all proposals were submitted and, if not, to get feedback as to why the vendor(s) did not submit its proposal. Regarding the Task Order 6 Procurement Record in the file, [redacted] acknowledged [redacted] "oversight" on [redacted] part that the record did not capture relevant information for the record. The "Proposal" part of the record did not include RFQ's amended proposal information and its new, extended due date, [redacted], 2018. Without having a properly completed Procurement Record for [redacted] review, [redacted] could not recall the specific purpose of his [redacted] 2018 email. [redacted] explained that the record was approved electronically in CLM.

OIG Recommendations

The WMATA Procurement Procedures Manual provides, among others, values and principles for having effective, professional customer service and for maintaining complete procurement records.[4] The guiding principles promote Procurement staff to be a resource and partner to our customers and to maintain complete procurement records. In this instance, the Procurement Record kept an incomplete record of its proposal information. In addition, albeit the vendor is responsible for updating its POC information, WMATA collectively gave an impression of having a lax environment by not returning phone calls or respond adequately to email inquiries. To that end, OIG makes the following recommendations:

1. Management should ensure that Procurement Records accurately capture and maintain a record of appropriate procurement activities in the CLM system.

[4] Procurement Procedures Manual (Version 7.4), August 2017, pg. vi.

2. Remind staff to consistently maintain their professional relationships with customers by responding to their phone calls and email contacts so inquiries are adequately addressed.

Please provide a response to OIG's recommendations by May 3, 2019.

cc: COUN – [redacted]
IBOP – [redacted]

M E M O R A N D U M

SUBJECT: Management Alert
Procurement of 8000 Series Railcars (MA-19-0001)

DATE: April 23, 2019

FROM: OIG – Geoffrey A. Cherrington PARP Ex. 6.1.6

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) conducted a review to identify the most serious challenges that WMATA faces in the procurement of the 8000 series railcars. This Alert does not identify actions to be taken, but, is provided for information to assist in the procurement process.

As part of this review, OIG contacted the Massachusetts Bay Transit Authority (MBTA), Southeastern Pennsylvania Transportation Authority (SEPTA), and Los Angeles County Metropolitan Transportation Authority (LACMTA) to identify challenges and lessons learned from their procurements of their next generation railcars.

All three of these transit agencies awarded the manufacturing of their next generation railcars to CRRC Corporation Limited (China Railway Rolling Stock Corporation) formerly known as Changchun Railway Vehicles Company, a Chinese state owned rolling stock manufacturer. The largest rolling stock manufacturer in the world, CRRC was formed on June 1, 2015, with the merger of China CNR Corporation and CSR Corporation Limited.

The primary reasons for the awards to CRRC, according to these transit agencies, was CRRC had the highest-rated technical offer and lowest price while offering the most robust U.S local employment programs. CRRC manufactures the exterior shells in one of its factories in northeastern China, while the final assembly will be completed in Springfield, Massachusetts. CRRC plans to invest in a Los Angeles-based facility to manufacture major components including propulsion and air-conditioning.

The emergence of the Chinese into the transit railcar rolling stock market in the U.S. is relatively new. MBTA awarded a $566 million contract to CRRC in 2014 to build roughly 404 new railcars by 2020. A second order was awarded in 2016 for 120 new cars to begin in 2022, making the total contract award amount $842 million.

CRRC purchased and rehabilitated a $95 million, 204,000 square foot railcar manufacturing facility; a 2,240 foot dynamic test track, and a staging and storage area in Springfield, Massachusetts, where assembly of the railcars takes place. CRRC estimated that this plant, when fully operational, would create roughly 200 new jobs in Springfield, Massachusetts.

In 2017, SEPTA awarded a $137.5 million contract to CRRC Massachusetts (MA), the American subsidiary of China Rolling Stock Corporation. The contract includes an option for an additional 10 cars for $24.5 million.

During 2017, LACMTA awarded a $647 million contract to CRRC to build 346 railcars. The first 218 cars are to be delivered by 2020 and the remaining 64 cars by September 2021.

Reuters reported on March 27, 2017, "that CRRC has been steadily gaining ground in the U.S. market. The company had won a $567 million Boston contract in 2014, and another bid worth $1.3 billion in 2016 to build railcars in Chicago." The Boston and Chicago awards were prior to the awards to SEPTA and LACMTA. To date, CRRC has been awarded five contracts in the U.S. totaling approximately $3 billion.

A Washington Post article, dated January 7, 2019, raised concerns about the Chinese threat faced by WMATA if its next generation railcars are procured by CRRC and the resulting potential risks to the U.S. and Its critical transit infrastructure resulting from cyberattacks directed by the Chinese.

On the heels of the Washington Post article, The House of Representatives, Committee on Homeland Security, Subcommittees on Cybersecurity, Infrastructure Protection and Innovation and Transportation and Maritime (116th Congress) held joint hearings on February 26, 2019, regarding securing U.S. surface transportation from cybersecurity attacks. A transportation cybersecurity expert from the Rail Security Alliance provided testimony concerning their assessment of the potential cyber threat risks facing the U.S. from procuring rolling stock from China. According to the testimony of Eric R. Olson, Vice President of the Rail Security Alliance, "Using state-backed financing, subsidies, and array of other government resources, CRRC has strategically targeted and sought to capture the U.S. railcar manufacturing sector."

On March 19, 2019, a bipartisan group of Senators, sponsored by U.S. Senators John Cornyn (R-TX) and Tammy Baldwin (D-WI) introduced the Transit Infrastructure Vehicle Security Act, which would prevent federal funds from being used by transit agencies to purchase railcars or buses manufactured by Chinese government owned, controlled, or subsidized companies. Senate Banking, Housing, and Urban Affairs Committee Chairman, Senator Mike Crapo (R-ID), and Ranking Member, Sherrod Brown (D-OH), are original cosponsors of the legislation.

"China poses a clear and present danger to our national security and has already infiltrated our rail and bus manufacturing industries," Senator Cornyn said. "The threat to our national security through the exploitation of our transportation and infrastructure sectors is one we should take seriously. This legislation will help safeguard against this threat, and I'm thankful for the support of my colleagues."

"China has made clear its intent to dismantle U.S. railcar manufacturing in its 'Made in China 2025' plan—our economic and national security demands that we address Chinese attempts to dominate industries that build our nation's critical infrastructure," said Senator Baldwin. "That's why I'm joining my colleagues on both sides of the aisle to introduce legislation to hold China accountable because we need to do all we can to support American workers and American-made products."

"This strong bipartisan bill protects federal dollars from being spent on Chinese buses and railcars, and, improves cybersecurity in public transportation," said Senator Brown. "Federal dollars should not support Chinese state-controlled enterprises that want to undermine U.S. manufacturers and overtake our supply chain that supports rail and bus manufacturing."

This Act as proposed would ban Federal funding being spent for Chinese manufactured railcars and buses. It would also penalize transit agencies for the use of non-Federal funding to purchase Chinese manufactured railcars and buses even if done solely with the agency's non Federal dollars which could cause transit agencies to lose all of their Federal and state of good repair mass transit dollars for the fiscal year non-federal funding is used under 49 U.S.C.§ 5337.

However, agencies like MBTA, CTA and LACMTA which already have signed contracts to purchase Chinese railcars will be able to issue new contracts making subsequent purchases.

Understanding the potential risks associated with procuring railcars from foreign manufactures, OIG identified the following challenges and lessons learned from MBTA, SEPTA and LACMTA which are applicable to any future railcar procurement regardless of the manufacturer selected.

PARP Ex. 6.1.4

[redacted]

OIG is concerned about the selection process to award the contract to the manufacturer who will build the new railcars for WMATA. The contract award process needs to include a robust vetting process of all competing vendors given the heightened media attention and Congressional concerns that have been expressed regarding the risk for selecting CRRC. WMATA will also need to be actively engaged in program management and quality control oversight during all aspects of the manufacturing process. In addition, cyber risk mitigation will be even more critical for WMATA to provide oversight to ensure sufficient cyber risk mitigation processes are being followed to mitigate threats, if CRRC is awarded the contract.

OIG is concerned that the technology on the railcars and rail systems could be compromised by the Chinese who possess cyber technologies that they will increasingly unleash on U.S. companies, the military, election systems and critical infrastructure posing a significant threat to national security, according to Dan Coats, Director of National Intelligence (DNI) who told the Senate Intelligence panel in an annual hearing during April 2019 called Worldwide Threat Assessment. WMATA railcars travel in close proximity to the White House, Capitol Hill, The Pentagon, a major domestic airport, and soon a major international airport. This could allow the railcars to be used as platforms to gather intelligence regarding critical transportation infrastructure patterns and cell phone activity if critical onboard rail technology is not continuously monitored to mitigate technology threats.

Another major concern is that any disruption of Metro service resulting from cyberattacks directed by the Chinese or any other foreign actor would have significant impact to the potential safety and confidence of the commuting public and could cause mass disruption.

OIG suggests that these concerns be a factor in the selection of a manufacturer of the 8000 series railcars.

M E M O R A N D U M

SUBJECT: Management Alert

DATE: May 23, 2019

FROM: OIG – Geoffrey A. Cherrington

Geoffrey Cherrington [redacted] WMATA

TO: GMGR – Paul J. Wiedefeld

RE: 19-0393-C Data Sensitivity Violation

The Office of Inspector General (OIG) is transmitting this Management Alert to update you on the recent discovery of sensitive Washington Metropolitan Area Transit Authority (WMATA) documents on a Red Line train.

On [redacted] 2019 at [redacted] OIG personnel boarded a Red Line train at Judiciary Square bound for Shady Grove Metro Station. Upon entering the first car of the train, OIG personnel discovered several WMATA documents on an unoccupied seat. These documents included technical schematics for [redacted], an [redacted] Training Manual, and [redacted] procedures (see attached). These documents were secured by OIG personnel and will be delivered to [redacted]

WMATA P/I 15.12/2 – Data Sensitivity, §3.09 defines Sensitive Data as "*any data in print or electronic form of which a compromise of confidentiality, integrity, or availability would have a material adverse effect on Metro's interests, the conduct of Metro's business or the privacy to which individuals are entitled.*" P/I 15.12/2, §5.01 further establishes four sensitivity levels assigned to WMATA data. [redacted] WMATA P/I 15.12/2, §5.06(g) further indicates all "paper documents and files containing sensitive information should be secured at all times." This P/I applies equally to employees and contractors.

cc: COO – J. Leader
COUN – P. Lee

[1] [redacted] is a term referenced in both the [redacted] manuals

INCP – E. Christensen

Attachments

M E M O R A N D U M

SUBJECT: Management Alert DATE: July 9, 2019

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

RE: 20-0003-I Non-Compliance w/Licensing Regulations

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding violations of jurisdictional regulations governing the use of electronic seals and/or signatures for PARP Ex. 6.1.6 During the course of a related investigation, the OIG learned [redacted] in the PARP Ex. 6.1.6 were providing unlicensed individuals access to and responsibility for affixing the licensee's electronic seals and signatures to WMATA certification documents. This activity could compromise the safety of WMATA employees and customers.

Regulations for Maryland allow a licensed [redacted] who prepares and/or approves documents to use electronic seals and/or signatures provided that those electronic seals/signatures are under the "exclusive control of the licensee using it."[1] Virginia and DC have similar regulations governing the use of electronic seals and/or signatures. Virginia allows for the use of electronic seals and signatures when "it is under the professional's direct control."[2] DC allows for the use of a [redacted] digital signature, provided the digital signature is under the "[s]ole control by the person using it."[3]

OIG contacted licensing officials in the respective jurisdictions regarding the electronic sealing and signing regulations. Maryland Department of Labor's Licensing Board Counsel advised that, while they were unaware of any prior instances involving individuals other than the licensee having access to the licensee's stamp (seal), their "first impression" was the licensee was "treading on dangerous waters" by relinquishing control over his/her stamp. They were also "very leery" of individuals other than the licensee having access to a [redacted] "private key" to the stamp.[4] DC's Board Administrator for PARP Ex. 6.1.6 indicated

[1] Section 09.23.03.09 E(2)(b)(ii) of Code of Maryland Regulations (COMAR). The reference to digital and electronic seals and signatures is utilized interchangeably in this document.

[2] Title 18 Section 10-20-760 of Virginia's Administrative Code, which also applies to PARP Ex. 6.1.6

[3] DC Municipal Regulation 17-1516.10(a)3. Regulation 17-1516.9 provides for the placement of either a digital signature or handwritten signature adjacent to or across the computer generated seal.

[4] The OIG believes access to the "private key" refers to access to the electronic seal

it was impermissible for individuals other than the licensee to maintain or affix his/her digital seal and signature. The Board Administrator added, "The seal should have the sole control by the person who owns it." The OIG attempted to obtain a written opinion from Virginia concerning its regulation with respect to the electronic sealing and signing requirements, but has not as of this writing received a response.

The OIG discussed concerns over [redacted] apparent lack of compliance with jurisdictional regulations in this regard with [redacted] indicated [redacted] implemented an approval process several years ago for the application of licensed WMATA [redacted] electronic seals and signatures in the review, approval, and certification of documents. [redacted] developed forms documenting the unlicensed individual's preparation and review, and the licensee's subsequent review and approval of the document(s) being certified. Following the completion of the approval document(s), the unlicensed individual applies the licensee's electronic seal and signature to certify the WMATA document(s). The electronic seal and signature are stored electronically on a cloud platform. There is no internal control preventing an individual from affixing the licensee's electronic seal and signature on documents without review by the licensed [redacted].

[redacted] efforts attempted to achieve some level of internal control over the application of electronic seals and signatures by individuals other than the licensed professional certifying WMATA's documents. However, despite [redacted] efforts, the fact remains that this practice violates jurisdictional regulations since licensees do not have exclusive or sole control over their electronic seals and/or signatures. The aforementioned practice also does not prevent improper certification of WMATA documents that have not been reviewed or approved by the licensee, as the unlicensed employee has unrestricted access to the licensee's electronic seal and signature through the cloud. The OIG did not perform any comparison of WMATA documents certified through the non-licensee's application of electronic seals and signatures to the approval forms developed by [redacted] The OIG remains concerned, however, over the possibility that [redacted] could have been certified without the requisite review and approval by the licensed [redacted] thereby compromising the safety of customers and employees.

This Management Alert is being provided so that immediate appropriate action can be taken to safeguard employees and customers, provide notice of non-compliance if required by the aforementioned regulations, and to ensure [redacted] and other WMATA departments are in compliance with jurisdictional [redacted] regulations going forward.

cc: COUN – P. Lee
INCP – E. Christensen
COO – J. Leader

M E M O R A N D U M

SUBJECT: Management Assistance Report
Concerns with Transformers (MAR-20-0009-I)

DATE: February 28, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Assistance Report to elevate potential safety and service disruption concerns associated with transformers installed during the PARP Ex. 6.1.4 .[1]

BACKGROUND

The Office of Infrastructure Renewal Program (IRPG) managed the replacement of seven transformers at three traction power substations PARP Ex. 6.1.4 under Contract PARP Ex. 6.1.4 during PARP Ex. 6.1.4.[2] The contract required that transformers be manufactured by PARP Ex. 6.1.4 specified manufacturers or an approved equal. Contract PARP Ex. 6.1.4 was awarded to PARP Ex. 6.1.4 PARP Ex. 6.1.4 is the manufacturer of the transformers being supplied under this contract.[3] In addition to the seven transformers installed during PARP Ex. 6.1.4, Contract PARP Ex. 6.1.4 calls for the installation of PARP Ex. 6.1.4 additional PARP Ex. 6.1.4 transformers.[4]

CONCERNS

Following the installation of the PARP Ex. 6.1.4 transformers during PARP Ex. 6.1.4 review of design and shop drawings determined incorrect current transformers (CTs) were installed in these transformers.[5] CTs are internal components inside the overall transformer. PARP Ex. 6.1.4 dispatched staff to the PARP Ex. 6.1.4 substations to replace the CTs, which required the opening and partial draining of oil from the PARP Ex. 6.1.4 transformers. At management's request, PARP Ex. 6.1.4 agreed to PARP Ex. 6.1.4 .

---

[1] PARP Ex. 6.1.4

[2] Contract PARP Ex. 6.1.4 includes other components for upgrading the Blue Line rail power system.

[3] PARP Ex. 6.1.4 was PARP Ex. 6.1.4 transformer manufacturers specified in the IFB. PARP Ex. 6.1.4

[4] PARP Ex. 6.1.4 of these transformers have already been installed at PARP Ex. 6.1.4 substations PARP Ex. 6.1.4 but not yet energized.

[5] CTs are internal components of the transformers, which serve as a metering instrument for the winding temperature indicator.

The PARP Ex. 6.1.4 transformers at the PARP Ex. 6.1.4 were placed into service for a seven-day "burn-in" period, commencing PARP Ex. 6.1.4, 2019. On PARP Ex. 6.1.4 2019, one of these transformers experienced a failure, resulting in significant damage. Despite testing while at the PARP Ex. 6.1.4, the root cause could not be determined.

The failed transformer was transported to PARP Ex. 6.1.4 headquarters in PARP Ex. 6.1.4 to facilitate a comprehensive inspection and root cause analysis by WMATA's third-party consultant, PARP Ex. 6.1.4[6] PARP Ex. 6.1.4 root cause analysis identified inconsistent crimping procedures and other concerns with the workmanship of the failed PARP Ex. 6.1 transformer. However, PARP Ex. 6.1 opined the transformer failure "may have been caused by human error during CT replacement and may be considered as an isolated failure." Some of the WMATA technical staff OIG interviewed were not in full concurrence with PARP Ex. 6.1.4 conclusion.

A different PARP Ex. 6.1 transformer installed at the PARP Ex. 6.1.4 during the same PARP Ex. 6.1.4 experienced significant issues following energization. Excessive negative pressure readings and excessive moisture resulted in WMATA taking this PARP Ex. 6.1 transformer out of service on PARP Ex. 6.1.4 2019, approximately PARP Ex. 6.1.4 after being energized. This PARP Ex. 6.1 transformer remained out of service for almost PARP Ex. 6.1.4 before being returned to service at the end of PARP Ex. 6.1.4 2019.

The OIG investigation also found that CT circuits on the PARP Ex. 6.1.4 recently installed PARP Ex. 6.1 transformers still have not been tested. As a result, these transformers are operating without winding temperature protective circuits enabled as a first line of protection, the absence of which could result in substantial damage in the event of even a low-level fault.

The OIG review of various WMATA records revealed longstanding safety and reliability issues with PARP Ex. 6.1 transformers, not limited to Contract PARP Ex. 6.1.4.[7]

- An PARP Ex. 6.1.4, 2007 internal memorandum described a PARP Ex. 6.1 transformer failure at PARP Ex. 6.1.4 that caused an electrical fire. An independent company performed a post-incident analysis, which identified irregularities in the transformer's connections, resulting in a short circuit. This document also indicated another PARP Ex. 6.1.4 transformer at this location was removed from service during the prior year after oil sample test results revealed internal electrical arcing.
- PARP Ex. 6.1.4, 2012 letter to WMATA acknowledged PARP Ex. 6.1.4
- PARP Ex. 6.1.4, 2012 email to WMATA indicated, in relevant part, PARP Ex. 6.1.4

[6] PARP Ex. 6.1 also performed a root cause analysis.
[7] OIG can provide source documents at Management's request.

- An [redacted] 2015 internal memorandum indicated that [redacted] supplied about [redacted] oil-filled transformers during years [redacted]. By 2012, [redacted] of them were operating abnormally, including one that had failed.... Due to poor quality control and transformer quality, WMATA Engineering is recommending that [redacted]" Management was unable to determine whether they took any action with respect to [redacted] as a result of this recommendation.

- The Maintenance of Way Engineering (MOWE) Director of Traction Power Operations' [redacted], 2019 email indicated, [redacted]

Despite the aforementioned concerns, WMATA has continued to accept [redacted] transformers on current and future projects. [redacted] will be supplying [redacted] additional transformers as part of Contract [redacted]. Additionally, [redacted] under construction is also being equipped with [redacted] transformers, similar to those being supplied through Contracts [redacted] and [redacted].[8]

The OIG is bringing these facts and circumstances to Management's attention for immediate action to ensure the continued reliability of train service and to safeguard the public and employees.

We recommend the General Manager/Chief Executive Officer consider the following actions to address the issues identified above:

[redacted]

Please provide a response to our recommendations by March 25, 2020.

cc: COUN – P. Lee
COO – J. Leader

[8] [redacted]

M E M O R A N D U M

SUBJECT: Management Assistance Report (MAR-20-0026-C)

DATE: April 3, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Assistance Report (MAR) to bring facts and circumstances to Management's attention for immediate action to ensure the continued safeguard of WMATA's employees, stakeholders and assets.

BACKGROUND

The OIG has received multiple complaints identifying fraudulent invoice phishing schemes targeting WMATA and its vendors. In one instance, a vendor who did not have a relationship with WMATA was led to believe it was conducting business with WMATA. Unfortunately, the vendor was dealing with an individual who was attempting to commit fraud. The schemes reported to OIG are described below.

FRAUD SCHEME ACTIVITY

The most recent incident was reported to the OIG in [redacted] 2020 by the PARP Ex. 6.1.6 [redacted] reported receiving a fraudulent email from someone representing himself to be with PARP Ex. 6.1.4 [redacted] which is a legitimate WMATA contractor. The email inquired about the status of outstanding invoices and requested WMATA change PARP Ex. 6.1.4 bank account information. The e-mail was sent from an address resembling PARP Ex. 6.1.4 legitimate e-mail address. [redacted] personnel believed the e-mail was a legitimate request and replied with an attached Electronic Funds Transfer (EFT) form for the recipient to update. The unknown email recipient submitted a modified EFT form for processing. [redacted] did not verify the request with personnel at PARP Ex. 6.1.4 .

On PARP Ex. 6.1.6, 2020, [redacted] submitted a payment request to Accounts Payable (ACCT) for two legitimate PARP Ex. 6.1.4 invoices totaling $126,571.44 ($63,285.72 each). On [redacted] 2020, payment in the amount of $126,571.44 was issued to the fraudulent account.

On [redacted] 2020, PARP Ex. 6.1.4 contacted [redacted] inquiring about outstanding invoices. PARP Ex. 6.1.4 confirmed they did not receive payment for their services and did not make a request to change their bank account information. [redacted] immediately notified ACCT to stop a third payment from being released.

On PARP Ex. 6.1.6, 2020, OIG was informed that all funds were recovered and there was no monetary loss to WMATA or the vendor. Further, ACCT has implemented a procedure requiring all requests for changes to banking information be submitted through the Vendor Portal.

In a second instance, the email account of PARP Ex. 6.1.4, a legitimate WMATA vendor, was compromised. An unknown individual posing as PARP Ex. 6.1.4 requested WMATA to change the bank account information on file. WMATA changed PARP Ex. 6.1.4 banking information and subsequently paid four legitimate invoices to the fraudulent bank account. Once notified of the error by the vendor, WMATA was able to reverse three of the four payments. One payment could not be reversed, which resulted in a PARP Ex. 6.1.4 loss to the vendor. The vendor is still pursuing WMATA for payment since they believe WMATA did not provide proper due diligence in researching the requested change.

In a third instance, a third-party posing as WMATA placed an order, via fax, to a restaurant supply company called PARP Ex. 6.1.4. This order included WMATA's tax exempt number, banking information, and the contact information for the ACCT Manager. PARP Ex. 6.1.4 believed the orders were legitimate and shipped the items to a non-WMATA location in Washington, DC. PARP Ex. 6.1.4 did not verify the orders with WMATA.

PARP Ex. 6.1.4 later contacted the ACCT Manager directly for payment. The ACCT Manager informed PARP Ex. 6.1.4 the invoices were fraudulent and refused payment. While WMATA did not incur a financial loss regarding this incident, the vendor could not recover the equipment delivered or payment from the third party.

OIG confirmed that WMATA's tax exempt number and banking information could easily be found on WMATA's website. After a coordinated effort by OIG, who informed the Chief Information Security Officer, (CISO), this information was removed from the external website and is no longer available to the public. In addition, OIG Special Agents visited the site where the items were shipped to obtain evidence regarding the individuals who picked up the supplies. OIG was not able to determine who picked up the items due to the length of time it took to discover the fraud.

The OIG is bringing these facts and circumstances to Management's attention for immediate action to ensure the continued reliability of WMATA's computer network and to safeguard the public and employees. OIG will be issuing the attached Fraud Awareness Bulletin to WMATA employees to bring awareness of this type of fraud and to ensure that these instances are promptly reported to the OIG, who is currently investigating these matters.

We recommend the General Manager/Chief Executive Officer take the following actions to address the issues identified above and limit WMATA's exposure to fraud:

1. Conduct a review of WMATA's public facing website and portals to ensure no sensitive information is posted electronically;

2. Put additional controls in place that will not allow staff responsible for paying vendors to change or alter payee financial information without supervisor approval and verification from the vendor after it is submitted through the vendor portal;

3. Provide periodic cybersecurity and fraud training to staff by OIG and ITCS to ensure they are aware of possible fraud schemes;

4. Instruct staff to report Electronic Fund Transfer (EFT), phishing schemes and other financial fraud attempts in a timely manner to ITCS and then to OIG;

5. Validate vendor information on a periodic basis; and

6. Address responsibilities and liability issues if a vendor becomes compromised to understand the impact on WMATA.

This matter is being forwarded to you for review and action as appropriate. Please respond, in writing, by May 3, 2020, documenting any actions planned or taken.

Attachment

cc: CFO - D. Anosike
COUN - P. Lee
IBOP - J. Kuo
CIO - A. Short
COO - J. Leader
ITCS - K. Malo
PRMT - S. Moore

M E M O R A N D U M

SUBJECT: Management Assistance Report (OIG-20-0173-C)

DATE: May 27, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Assistance Report to inform you of serious shortcomings in WMATA's handling of a recent cybersecurity intrusion associated with Russian internet protocol (IP) addresses, weaknesses in some of WMATA's cybersecurity practices, and obstacles OIG encountered in investigating the intrusion in question. In particular, OIG found that:

- The intrusion occurred on devices that had not been patched or updated for more than a year and that were beyond their end-of-life in any case.
- WMATA has not clearly defined who is responsible to apply critical patches on network devices.
- WMATA lacks adequate procedures to assure that devices beyond the end-of-life are timely replaced.
- Responsible WMATA offices did not timely inform OIG about the intrusion, have provided inconsistent and contradictory information to OIG, and to date have failed to provide requested information that OIG requires to complete its investigation.
- As a result, OIG to date has been unable to establish basic facts, such as the extent of the intrusion and what precisely was done to mitigate it.

The WMATA Compact directs OIG to conduct and supervise investigations relating to WMATA activities. The Compact makes no exceptions for IT activities or cybersecurity incidents. Even if several offices are involved in an investigation, as may happen in the case of cybersecurity incidents, the Compact calls on OIG to supervise the investigation. OIG's investigation of the present matter continues. This report recommends immediate actions that OIG believes are needed to help protect WMATA's network against cyber threats.

Key OIG Findings

- On PARP Ex. 6.1.6, 2020, the WMATA Office of Cybersecurity Operations (ITCS) was notified that WMATA was at risk because it was running vulnerable versions of the PARP Ex. 6.1.4

- In fact, an actual intrusion occurred at least as early as PARP Ex. 6.1.6, 2020, in the form of outbound traffic through the PARP Ex. 6.1.4 to IP addresses associated with Russian sources. According to the FBI, this is part of a larger foreign-based scheme identified in multiple locations throughout the United States. Also, since OIG was provided limited logs, we could not confirm that there was no lateral movement impacting other devices, systems, or applications.

- ITCS has provided some information stating that the intrusion was detected on PARP Ex. 6.1.6 but has not said by whom. ITCS has provided other information reflecting that neither ITCS nor the contractor co-managing WMATA's Security Operations Center (SOC) detected the intrusion until PARP Ex. 6.1.6, 2020, 12 days after the fact.

- In response to the PARP Ex. 6.1.6 vulnerability notice, ITCS requested the PARP Ex. 6.1.4 administrator to apply system patches. ITCS did not approve the patches until PARP Ex. 6.1.6, 2020. The patches were unsuccessful because ~~the~~ PARP Ex. 6.1.4 ~~had~~ already been compromised.

- [redacted] had declared the compromised PARP Ex. 6.1.4 beyond the "end of life" in 2018. WMATA had last patched or updated them in [redacted] 2018. In [redacted] 2019 WMATA purchased four new PARP Ex. 6.1.4 to replace the outdated ones. However, they did not install them until after the intrusion was discovered and the attempted patch on the outdated devices failed.

- On PARP Ex. 6.1.6, 2020, ITCS for the first time notified OIG of this incident, reporting to us the PARP Ex. 6.1.6 vulnerability notice and stating that the intrusion had been discovered on PARP Ex. 6.1.6 As noted above, ITCS provided other conflicting information that the intrusion was discovered later.

- In the course of OIG's investigation, ITCS provided other incomplete and conflicting information that prevented OIG from determining all the relevant facts. This includes incomplete logs, precisely how and when ITCS fixed the vulnerability, and whether all affected WMATA devices were made available for forensic examination. The FBI Cybercrimes Task Force and the Department of Homeland Security (DHS) Cybersecurity Infrastructure and Security Agency (which OIG brought into the investigation) concluded that they had not received all the necessary drives for each device and could not reconstitute the devices based on the number of drives they did receive.

- Neither ITCS, the Office of Procurement (PRMT), nor the SOC contractor were able to provide OIG a fully executed copy of the contract signed by both WMATA and the contractor. This contract is critical to WMATA's cybersecurity. It obligates the contractor to provide managed security services protecting WMATA's entire network.

- ITCS notified both MTPD and OIG of the intrusion but failed to tell either that the other had been notified. As a result, OIG and MTPD reported the matter to two different FBI divisions. The Metropolitan Transit Police Department (MTPD) reported the intrusion to a division that does not investigate cybercrimes, potentially causing reputational harm to WMATA and delaying the investigation had OIG not discovered the lack of coordination.

OIG Authority to Conduct this Investigation

Under the WMATA Compact, Section 9(d), OIG is "an independent and objective unit of the Authority that conducts and supervises ... investigations relating to Authority activities; promotes economy, efficiency, and effectiveness in Authority activities; detects and prevents fraud and abuse in Authority activities; and keeps the Board fully and currently informed about deficiencies in Authority activities as well as the necessity for and progress of corrective action." There are no limitations on the types of "Authority activities" that OIG is authorized to investigate, and no exceptions for IT activities or cybersecurity incidents. Furthermore, the Compact makes clear that OIG has supervisory authority over investigations of "Authority activities" within WMATA, even if other elements or entities participate in the investigation. **(Exhibit 1)**

While ITCS plays a crucial role in protecting the network and is the first line of defense against cyber threats, once an intrusion is detected ITCS has a duty under WMATA policies to report it to OIG "at the earliest possible opportunity" **(Exhibit 1)**. OIG then has a duty to investigate it, and to coordinate with other investigative agencies such as the FBI and DHS as needed. The Compact and WMATA policies discussed in Exhibit 1 make this clear. OIG supervises efforts to assess the extent of the intrusion, to identify who perpetrated it, and to identify potential criminal activity. OIG also has a duty to evaluate the adequacy of remedial measures. OIG's role is consistent with practices in the federal government, where it is common for OIGs to be notified of cyber threats and incidents so that they can coordinate with all relevant agencies in applying proper investigative techniques and forensic analyses. It is important to WMATA for OIG to exercise its authority with full cooperation from all offices because OIG agents are trained in preserving evidence, maintaining a proper chain of custody that courts will accept, evaluating the significance of evidence gleaned from affected devices and associated electronic records, and testifying about our findings.

Investigation Summary

On PARP Ex. 6.1.6 2020, ITCS reported to OIG that it had detected an intrusion on a [redacted] A PARP Ex. 6.1.4 is a computer network device that often helps perform common tasks. As a result of the notification, OIG opened an investigation and contacted the FBI's Cybercrimes Task Force. At some point during the investigation, OIG learned from the MTPD that ITCS had also reported the intrusion to them. While it was appropriate to report the matter to both MTPD and OIG, ITCS never advised OIG that it had also reported the intrusion to MTPD. The lack of coordination caused both OIG and MTPD to report the matter to two different FBI divisions. MTPD reported the intrusion to the FBI's Joint Terrorism Task Force, which does not investigate cybercrimes, potentially causing reputational harm to WMATA and delaying the investigation had OIG not discovered the lack of coordination. When questioned, ITCS personnel said they forgot to disclose the MTPD notification to OIG.

While our investigation is still open, to date, OIG has been unable to complete it because we have not received sufficient information concerning the compromise. As a result, OIG thus far cannot ascertain if ITCS adequately preserved the evidence, determined who was behind the intrusion or effectively eliminated the vulnerability. OIG's investigation remains open until we can ascertain further information about the compromise.

As soon as OIG learned of the compromise, we sent an email to Internal Business Operations (IBOP) personnel advising them that OIG had opened an investigation and requested that they preserve all evidence.

OIG's investigation determined, among other details, that ITCS was initially notified of the vulnerability by the Center for Internet Security (CIS), Multi-State Information Sharing and Analysis Center (MS-ISAC) on PARP Ex. 6.1.6 2020. MS-ISAC advised ITCS personnel that it became aware, through a trusted third party, that WMATA was running vulnerable versions of PARP Ex. 6.1.4. In response to the notification, ITCS initiated action by requesting system patches to be completed by the PARP Ex. 6.1.4 administrator. ITCS did not approve the patches until PARP Ex. 6.1.6 2020. The patching was unsuccessful, as the PARP Ex. 6.1.4 were already compromised. The vendor did not release a security fix to remediate this vulnerability until PARP Ex. 6.1.6 2020.

WMATA purchased new PARP Ex. 6.1.4 in PARP Ex. 6 2019 because the existing PARP Ex. 6.1.4 were declared beyond the "end of life" (EOL) by PARP Ex. 6.1.4 in 2018. The Office of Infrastructure and Operations (ITIO), the division that purchased the new devices, did not install them upon purchase and could not explain why they did not install them, nor why the system was last patched in 2018.

During this investigation, OIG identified areas of concern as follows:

1. Lack of information provided to OIG by ITIO and ITCS regarding device ownership;
2. Poor governance over timely system patching and replacement of assets;
3. Inability to provide OIG with a signed contract for WMATA's managed security services (MSS) contractor;
4. Lack of transparency with the OIG on steps taken to remediate the intrusion and failure to provide relevant information;
5. ITCS's lack of understanding or clarity on how many devices were involved in the incident;
6. Lack of procedures to safeguard devices as evidence;
7. Failure to either maintain or provide OIG complete logs; and
8. Insufficient staff and tools to detect intrusions and other vulnerabilities.

In the remainder of the report, we detail the investigation to date and how these concerns have hampered OIG's efforts.

OIG Investigation – Detailed Analysis and Results

On [redacted] 2020, OIG received an email from ITCS that read, in part, as follows: **(Exhibit 2)**

Summary

On [redacted] *2019, the outbound traffic going to IP addresses associated with* [redacted] *, a critical vulnerability in* [redacted] *was detected. This vulnerability allows an attacker to gain unauthorized access to published applications and other internal network resources from the* [redacted] *servers, and eventually lead to a remote code execution.*

Announcement of this vulnerability was made in [redacted] *2019, along with recommended mitigation steps from* [redacted] *while the fix was on its way. On the* [redacted] *2020,* [redacted] *released firmware updates to address this vulnerability.*

Timeline

- [redacted] ***, 2019:*** [redacted] *posted a security bulletin about the vulnerability.*
- [redacted] ***, 2019:*** *Researchers determined at least 80,000 companies in 158 countries were potentially at risk. ITCS was notified of this vulnerability.*
- [redacted] ***2020:*** *WMATA outbound traffic to Russian IP addresses associated with the vulnerability was detected. A script called* [redacted] *was executed at 11:35AM and 9:11PM ET.*
- [redacted] ***2020:*** *Mitigation patches were applied to WMATA's* [redacted] *.*
- [redacted] ***, 2020:*** [redacted] *released firmware updates for affected* [redacted] *products.*
- [redacted] ***, 2020:*** *Ongoing investigations with key stakeholders to identify and remediate impact.*
  - *At 12:48 PM ET, a policy was created to drop any traffic on port 80 attempting to contact either of the original IPs associated with the vulnerability.*
  - *At 1:28 PM ET, it had been observed that the threat actor was performing port scans to find other available ports.*
  - *There was an emergency update scheduled for the* [redacted] *to permanently remediate the vulnerability.*

Business Impact

- *No current employee or customer impact. Suggests this attack is in the recon phase.*

This email did not identify who detected the traffic on [redacted] and why ITCS did not report it to OIG until 12 days later. When OIG inquired about the 12-day delay, ITCS stated that on [redacted], 2020, [redacted], their MSS contractor, traced the date of the intrusion back to [redacted], 2020. The email also did not disclose that the mitigation patches applied on [redacted] were unsuccessful.

Upon receiving the [redacted] email, OIG contacted the FBI, Cybercrimes Task Force, and later the DHS, Cybersecurity Infrastructure and Security Agency (CISA).

OIG confirmed [redacted] actions related to the intrusion by obtaining the service ticket dated [redacted], 2020. **(Exhibit 3)**

OIG also posed various questions related to the PARP Ex. 6.1.6, 2019 [redacted] security bulletin to PARP Ex. 6.1.4 and received the following information: **(Exhibit 4)**

1. What was the earliest date that your other clients notified you of the vulnerability and/or anomalies?

   PARP Ex. 6.1.6 *was the earliest date that a client told us that their* [redacted] *had been compromised (no IOCs / IOAs disclosed).*

2. WMATA advises, and I believe you confirmed, that on PARP Ex. 6.1.6 [redacted] posted a security bulletin about the vulnerability. How and when di [redacted] first learn of the PARP Ex. 6.1.6 [redacted] bulletin? Did [redacted] or [redacted] send that bulletin to WMATA or did WMATA otherwise get notice of it at the time [redacted] issued it? When did the WMATA SOC receive it?" What, if anything, did [redacted] or WMATA do, to your knowledge?

   It is unknown if any individuals within WMATA regularly review PARP Ex. 6.1.4 *Posts from Twitter.*

   [redacted] *sent a formal advisory (attached) [Exhibit 3] on* PARP Ex. 6.1.6 *to clients regarding additional information available as the exploit was discovered to be attempted in the wild and a certain cryptocurrency campaign did affect some of our clients. I cannot confirm what specific recipients, if any, received the advisory within the WMATA SOC. Please note, however, that* PARP Ex. 6.1.6 *was the date of escalation of the* [redacted] *findings by* [redacted] *and I believe a phone call took place between WMATA and* [redacted] *on that date regarding the incident and disclosing what we understood about the situation at the time.*

3. Did WMATA advise you or your team that on [redacted], 2020, MS_ISAC advised them that they are running the vulnerability?

   Not that we are aware.

4. If they had, would that have made a difference in finding the intrusion sooner related to the Russian IP addresses?

   Possibly, but it is very unlikely. This depends heavily on what level of detail was provided by MS_ISAC and if the information would have been enough to create detection around the logs leveraged to detect the compromise. This also depends on proper timing with [redacted] */WMATA allocating proper resources in time to build, test, and deploy the necessary monitoring use case(s) between* PARP Ex. 6.1.4 *with the information provided.*

   From [redacted] *understanding, detection of the attack requires certain visibility at the web/ URL layer for inbound traffic. Additionally, command and control indicators related to the system compromise could be a number of types of IP addresses or URLs controlled by the attacker. Because of this, detection of the actual compromise, unless specifically down to the campaign level with the specific IOCs (indicators of compromise) can be challenging.*

5. Did WMATA communicate with you between PARP Ex. 6.1.6 about MS-ISAC's notification?

Not that I am aware with the individuals I have consulted that work with the contract.

During OIG's investigation, we found the following email dated PARP Ex. 6.1.6 2020, to ITCS staff that reads, in part, as follows: **(Exhibit 5)**

The MS-ISAC has been informed through a trusted third party that your organization is running vulnerable versions of PARP Ex. 6.1.4 *and/or* PARP Ex. 6.1.5 *. It has recently been observed that there is widespread scanning for* PARP Ex. 6.1.5 *This vulnerability allows unauthenticated remote attackers to execute commands (RCE) on the targeted server after chaining an arbitrary file read/write (directory traversal) flaw. Further exploitation can allow threat actors to gain a foothold inside the targeted networks (CRITICAL RISK) and conduct further malicious activity, such as spreading ransomware.* * **
There is currently no patch for this and PARP Ex. 6.1.4 *has released mitigation steps for* PARP Ex. 6.1.5 *which requires a number of direct commands through the interface to address the issue. Please also reference the provided open source article for additional information to determine if you have been compromised, mitigation steps for* PARP Ex. 6.1.5*, and proof of concept code.*

ITCS acknowledged the message by replying on PARP Ex. 6.1.6, 2020, "We need to investigate immediately." While there is evidence that ITCS was trying to mitigate the problem, we do not know why ITCS did not report the vulnerability to OIG on PARP Ex. 6.1.6 2020.

We also do not know why ITCS did not report the intrusion to OIG on PARP Ex. 6.1.6 despite stating in its PARP Ex. 6.1.6 email that the intrusion was discovered on PARP Ex. 6.1.6. Also, if neither ITCS nor PARP Ex. 6.1.4 discovered the PARP Ex. 6.1.6 intrusion until PARP Ex. 6.1.6, we do not know why 12 days passed before they detected it. All events on WMATA's network pass through the SOC. WMATA and PARP Ex. 6.1.4 co-manage the SOC. The contract requires PARP Ex. 6.1.4 to provide managed security services in the form of co-managed security incident event management (SIEM) 24 hours a day, 365 days a year. Event logs are generated simultaneously with the underlying events. The central purpose of SIEM is to detect cybersecurity incidents as soon as they occur, through 24x7x365 monitoring of event logs by trained individuals.

On PARP Ex. 6.1.6, 2020, OIG met with ITCS to discuss the coordination of cyber events. During the meeting, no one from ITCS ever disclosed that they had been advised by MS-ISAC that WMATA was running vulnerable versions of PARP Ex. 6.1.4. Had ITCS notified OIG, there would have been an opportunity to discuss options and coordinate the matter more effectively.

Despite inquiry, OIG also does not have insight into how ITCS mitigated the intrusion and the vulnerability that enabled it.

On PARP Ex. 6.1.6, 2020, OIG and ITCS met to discuss the cybersecurity compromise and initial response. OIG coordinated a second meeting with ITCS on PARP Ex. 6.1.6 2020, and included FBI Special Agents from the Cybercrimes Task Force to assist in assessing the incident.

During the meeting, ITCS explained the following:

1. WMATA's firewall detected malware and the IP addresses were marked with Russian information;
2. Three (3) hard drives were removed from three (3) devices and taken off-line;
3. The attack could lead to possible ransomware;
4. They found no evidence of any data extracted; and
5. They found no evidence of movement inside the system by the intruder(s).

OIG asked ITCS to identify how many devices were involved, which applications were running on the devices, and when the devices were last patched. ITCS stated there were three (3) devices with three (3) hard drives and they only supported VPN Virtual Desktop Infrastructure (VDI). Two (2) of the devices were located at the Jackson Graham Building (JGB) and one (1) backup at the Carmen Turner Facility (CTF).

Despite the above statements, OIG was given inconsistent information regarding the total number of devices, hard drives, and applications running on the devices. OIG was not given sufficient event logs that would provide evidence of activity. ITCS initially informed OIG that three (3) devices were taken off-line as a result of the incident. ITCS also reported to OIG that there were three (3) hard drives (one with each device). Through interviews, OIG was informed that there was a fourth device and a fourth hard drive involved in the incident. As of the date of this memorandum, ITCS has not provided a definitive response to the existence of the fourth device, nor has OIG recovered it.

ITCS agreed to provide OIG the original three (3) hard drives associated with the devices so that OIG could forensically examine each one. They also agreed to provide OIG with the event logs for the past twelve months. OIG intended to make forensically sound copies of the hard drives and event logs for the investigation and also provide them to the FBI to perform an independent forensic examination.

On PARP Ex. 6.1.6, 2020, ITCS provided OIG with two (2) hard drives and logs for PARP Ex. 6.1.6 2020. Upon further request by OIG, ITCS provided the third hard drive on PARP Ex. 6.1.6 2020. During our investigation, OIG requested the hard drive from the fourth device on PARP Ex. 6.1.6 2020, but never received it, nor has OIG received any additional event logs. Prior to turning over the hard drives on PARP Ex. 6.1.6, 2020, ITCS said that they would be providing OIG with a letter. The letter was addressed to the Inspector General and was from the Chief Information Security Officer stating~~, in part~~, the following: **(Exhibit 6)**

> *Enclosed please find documents and other information responsive to your request, as described further on the back of this letter. As the investigation is current and ongoing, please note that the documents and other information provided are necessarily preliminary and incomplete. In addition, the documents and other information provided are customarily and actually treated as confidential, private and/or privileged by WMATA. The documents and other information are provided to you on the condition that you treat such documents and information as confidential and do not release them to the public or any other third party.*

In response to the letter, OIG stated that "*OIG requested these hard drives and storage devices in connection with an ongoing investigation by OIG…. You are required to provide these items to OIG by WMATA P/I 13.4.1. … OIG does not accept or agree to any conditions that you purport to impose on OIG's receipt of these items.*" PARP Ex. 6.1.5 [redacted]

On PARP Ex. 6.1.6 2020, OIG contacted DHS CISA, to coordinate a call between OIG, ITCS, FBI, and DHS to discuss the incident. OIG provided copies of the PARP Ex. 6.1.4 hard drives and event logs to DHS for forensic examination and investigative assistance.

OIG, FBI, and DHS confirmed through their forensic examinations that the event logs were incomplete and only had limited activity for PARP Ex. 6.1.6. Furthermore, both the FBI and DHS advised OIG that they did not believe they had all the necessary drives for each device, and they were unable to reconstitute the devices based on the number of drives they received.

Based on OIG's forensic examination of the hard drives and limited event logs, we determined there was clear internet traffic between a WMATA device and the two (2) Russian IP addresses. OIG found a file with the Russian specific marking in the file. OIG found evidence of the associated file from the intrusion. This file was deleted and discovered in the unallocated space of the hard drive. Because ITCS only provided OIG with limited event logs, we could not determine the exact date of the intrusion, even though the file had a "last modified" date stamp of PARP Ex. 6.1.6, 2018, PARP Ex. 6.1.6. OIG was also not able to determine the extent of the intrusion. **(Exhibit 7)**

In trying to identify the roles and responsibilities of WMATA's MSS contractor, PARP Ex. 6.1.4 we requested a copy of the contract. Neither PRMT, ITCS, nor PARP Ex. 6.1.4 were able to provide a fully executed contract signed by both parties. ITCS did provide the Invitation for Bid (IFB), an unsigned copy of the Solicitation, Offer and Award form, and the Scope of Work. The IFB was dated PARP Ex. 6.1.6, 2018. Based on these documents, it is clear that this contract is critical to WMATA's cybersecurity. The contract obligates PARP Ex. 6.1.4 to provide managed security services for WMATA's entire network as a co-manager of WMATA's SOC.

OIG interviewed the staff member responsible for managing the devices and obtained the patching logs for the devices approved by the WMATA Change Control Board (CBC). OIG determined the following:

1. The devices had not been patched or updated since PARP Ex. 6 2018; **(Exhibit 8)**
2. A contract employee installed the devices in 2014 and no longer worked for WMATA; and
3. New devices had been purchased and available for installation since PARP Ex. 6 2019 but were not installed until after the vulnerability was exposed and the intrusion had occurred.

OIG was also told the following:

- There were four (4) PARP Ex. 6.1.4; two (2) in JGB and two (2) in CTF;
- ITCS was first notified of the compromise on PARP Ex. 6.1.6, 2020;
- ITCS staff were instructed not to make any changes until further notice;
- ITCS advised it would continue to monitor any intruder activities;
- ITCS installed the four (4) new devices at the end of the day on PARP Ex. 6.1.6, 2020;
- Hard drives were not replaced by ITCS; and
- One compromised device supported VPN, while the other maintained a more sensitive application called Password Manager. Without the fourth hard drive, complete event logs, accurate accounting of all involved devices, and forensic examination of all involved devices, OIG cannot determine the depth and width of the intrusion.

OIG interviewed ITIO personnel, who were not aware WMATA had purchased four (4) new PARP Ex. 6.1.4 in PARP Ex. 6.1 2019. These personnel also did not know why the new devices were not installed to replace the outdated PARP Ex. 6.1.4 as intended.

OIG inquired about WMATA's patching policy and was advised that the affected devices were last patched in July 2018. OIG was told by ITIO personnel that WMATA has a good process. They all must go through a rigorous CCB process for approval and testing. Also, ITIO did not know why patching was not performed after PARP Ex. 6 2018.

OIG asked who the owner of the PARP Ex. 6.1.4 was and an ITIO official said the devices belong to ITCS. Additionally, ITIO staff indicated that they were loaning out staff to help ITCS manage these systems. ITCS advised OIG that the devices were owned by ITIO. When asked, ITIO did not know what applications run on the PARP Ex. 6.1.4. An ITIO staff member indicated that the devices only supported the VPN VDI. When OIG informed the staff member that there were four (4) or five (5) applications running on the PARP Ex. 6.1.4, including one of the more sensitive applications called Password Manager, the staff member opined that IT is significantly short-staffed.

OIG asked ITIO if it receives any security alerts for vulnerabilities. ITIO indicated it does not, but ITCS does. When asked who should have submitted the request for patching the NetScalers, ITIO stated it is ITCS's responsibility as the owner of the devices.

OIG is concerned about the lack of information and transparency related to this incident. We examined emails between ITIO and ITCS that contradict information provided to OIG. To date, OIG has not been provided the fourth device and is still not sure whether or not a fourth device exists. If the device does exist, we are concerned that it has not been adequately safeguarded for evidentiary purposes.

OIG is bringing the facts and circumstances of this incident to management's attention for immediate action to ensure WMATA's computer systems are safeguarded against cyber threats. The facts and circumstances are being provided in the hope that future incidents are handled with transparency so that both OIG and ITCS can better coordinate these matters. Ultimately, it is WMATA's stakeholders who are at risk.

Recommendations

We recommend the General Manager/Chief Executive Officer take the following actions to address the issues identified above:

1. Require ITCS to produce the fourth device if it exists, so that OIG may complete its investigation.

2. Require ITCS to produce the logs requested by OIG.

3. Require ITCS and ITIO to clearly define roles and responsibilities for managing patches for all WMATA's systems.

4. Require ITCS to provide timely notification of vulnerabilities detected to all system owners and stakeholders as part of WMATA's cybersecurity incident management process.

5. Require ITCS and ITIO to update WMATA's patch management process to include the use of automated patch management tools and utilities to assist in the timely identification and mitigation of vulnerabilities.

6. Require system owners to create an inventory of what applications run on each system and identify those with sensitive applications and data and provide this information to ITCS.

7. Require ITIO to implement an automated asset management system to timely track end-of-life and end-of-support of WMATA's hardware and software.

8. Require all network logs to be retained for at least 18 months to be able to discover and trace the origination of an intrusion.

9. Require ITCS and ITIO to develop procedures that include timely reporting and transparency to the OIG of cybersecurity vulnerabilities and cybersecurity incidents.

M E M O R A N D U M

SUBJECT: Management Alert
Web Content Filtering Concern (20-0008-I)

DATE: September 17, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding the effectiveness of WMATA's web content filtering system in preventing access to and transmission of objectionable and/or illegal material through WMATA networks. In four recent OIG investigations, employees were found to have been using WMATA-issued electronic devices and/or WMATA's network in violation of WMATA's electronic access usage policy.[1]

WMATA policy prohibits use of information technology systems to access inappropriate web content. The policy states that web content filtering techniques are used to examine and restrict incoming/outgoing prohibited content, including but not limited to "sexually explicit and obscene material (including any and all forms of pornography, adult humor, profanity, dating services/personals)."

OIG is bringing this matter to your attention in an effort to ensure that these restricted activities may be detected to protect WMATA's network and to identify possible crimes from being committed in the future. OIG has closely coordinated this effort with the Office of Cybersecurity to ensure that both our offices are jointly focusing on the matter.

The below listed OIG investigations have identified shortcomings in the current web content filtering protocol that may expose WMATA to significant risk.

1. An employee used a WMATA-issued cell phone to receive and store several pornographic video files without detection.[2] WMATA pays for all WMATA-issued cell phones to have data plans through PARP Ex. 6.1.5 cellular network. The circumstances demonstrate employees' ability to violate WMATA policy by bypassing the web content filtering protocol through the PARP Ex. 6.1.5 network.

2. An employee[3] used WMATA-issued computers, laptops, and a cell phone to access adult dating websites and solicit sex from a minor, for which PARP Ex. was eventually criminally convicted.

[1]WMATA P/I 15.3/4 Electronic Access Usage Policy – 5.06 Inappropriate Web Content and Filtering.
[2]This individual is no longer employed by WMATA.
[3]This individual is no longer employed by WMATA.

3. Forensic analysis of WMATA-issued devices seized during the investigation revealed over 900 saved pornographic files and significant activity on numerous pornographic websites. OIG referred these files to federal law enforcement authorities to determine whether the material included illegal child pornography. No child pornography was found.

   While most of the pornography was accessed/downloaded through private networks, the employee used at least one IP address associated with WMATA's network to access pornographic material. In some instances, the employee also used a WMATA-issued mobile hotspot device[4] without connecting to WMATA's Virtual Private Network (VPN)[5] to bypass web content filtering and access/download pornographic material undetected. There was evidence the employee utilized a WebKit[6] to bypass web content filtering protocol and obfuscate web browsing activity. OIG also determined the employee downloaded "peer-to-peer" file sharing software to a WMATA-issued device, which exposes WMATA's networks to significant malware vulnerabilities. This file sharing method is also known by law enforcement authorities to be a common method for transmitting child pornography and other illicit material.

4. An employee[7] used a WMATA-issued computer to store and, in some cases, solicit dozens of pornographic files from non-WMATA individuals. OIG observed instances where some of the pornographic material was embedded in emails originating from non-WMATA accounts and transmitted through WMATA email servers to the employee's work email account.

5. OIG identified an employee whose WMATA-issued computer contained evidence of at least 83 visits to pornographic websites. This employee also utilized a WebKit to bypass WMATA's web content filtering protocol and obfuscate web browsing activity. OIG also found evidence the employee installed tools on the WMATA-issued computer to facilitate access to the "dark web."[8] Specifically, the employee visited a known dark web market site on at least 22 occasions in the past several years. Dark web market sites sometimes contain illegal content that users may attempt to purchase anonymously.

OIG consulted with WMATA Department of Information Technology (IT) officials regarding current web content filtering protocol and oversight. IT's Office of Cybersecurity (ITCS) utilizes PARP Ex. 6.1.1 firewall devices, which include a standard web content filtering software package with content categories that can be restricted based on ITCS' specifications. ITCS renewed support for their existing PARP Ex. 6.1.1 firewall devices from PARP Ex. 6.1.4

WMATA employees who attempt to access restricted content through WMATA's network are supposedly redirected to an error screen featuring a notification that access is blocked due to restricted content. However, OIG learned ITCS is not alerted when such an attempt occurs. In addition, ITCS does not independently perform or receive PARP Ex. 6.1.1 trend analyses identifying suspect behavior such as, for example, when a single user makes repeated attempts to access restricted content. According to one ITCS official, OIG's inquiry was the only time of which PARP Ex was aware that a concern regarding access to restricted content had been raised.

---

[4] A portable electronic device that allows the user to connect multiple devices at one time, generally for a monthly service and/or data plan fee.
[5] A VPN is an encrypted internet connection from an external device to WMATA's network.
[6] An add-on/component to the Safari and/or Chrome web browser designed to allow the web browser to render web pages and may permit the user to browse anonymously.
[7] This individual is no longer employed by WMATA.
[8] Part of the internet that is not visible to search engines and requires the use of an anonymizing browser to be accessed.

OIG provided ITCS with an example from PARP Ex. 6.1.6 2018 in which one of the above employees used a WMATA IP address to successfully access a website called "Chaturbate – Free Adult Webcams." OIG believes this website to be pornographic in nature. ITCS was unable to determine why web content filtering failed to restrict access in this circumstance, because the PARP Ex. 6.1.1 product does not maintain web logs going back to that timeframe.

ITCS' research demonstrated that employees can use private networks to access restricted content undetected, even while using non-VPN. The ITCS official acknowledged the ability to screen all WMATA-issued devices for accessing restricted content regardless of geographic location warrants additional review, especially given the increased use of telework. The ITCS official noted that access to pornographic sites was especially concerning, describing those sites as "laden with malware" and a huge risk to WMATA's network.

In addition, ITCS currently has no capability to identify pornographic content being sent through WMATA's email system. While it is possible for ITCS to scan file attachment sizes for indicators of pornography transmission, this strategy may not be practical from a business standpoint. Likewise, ITCS has no insight into what content is being sent through WMATA-issued cell phones via PARP Ex. 6.1.6 data network. The ITCS official speculated that, while the technological capability for monitoring these networks may exist, those capabilities may not be cost efficient from a business standpoint.

OIG and ITCS agreed that pornography sites and user behavior represent a risk of exposure to viruses and malware. Hackers can use these sites as a trap to steal information from web users browsing websites. Cyber criminals can also use pornography as a lure to malware or a fraud scheme. The constant clicking through advertisements and content can increase the risk of installing malware. Also, given the embarrassment factor, this activity will likely go unreported by the employee.

OIG recommends management consider the following actions to address the issues identified above and to limit WMATA's exposure to associated cybersecurity, criminal, civil, and reputational risk:

1. Further assess areas of vulnerability for employees to bypass the current web content filtering protocol.
2. Identify where ITCS' current tools/capabilities can improve security in this regard with minimal expense.
3. Strengthen WMATA's network security in accordance with industry best practice to effectively prevent or identify:
   a. Access to websites containing pornographic or other restricted content, including dark web access;
   b. Use of WMATA email servers and WMATA-issued devices (i.e. cell phones, hotspots, etc.) to access and/or transmit pornographic or other restricted content; and
   c. Downloading of peer-to-peer file sharing software and tools enabling dark web access on WMATA-issued devices and infrastructure.
4. Develop and implement protocols to monitor, document, and report employee violations of electronic access usage policy for management's immediate action.

cc: COUN – P. Lee
IBOP – J. Kuo

M E M O R A N D U M

SUBJECT: Management Alert
RAIL Employee PARP Ex. 6.1.6
PARP Ex. 6.1.6

DATE: December 22, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate a safety concern regarding WMATA employee PARP Ex. 6.1.6. Recently OIG received a call from an anonymous individual alleging PARP Ex. 6.1.6 admitted to PARP Ex. 6.1.6 The caller said PARP Ex. 6.1.6 was PARP Ex. 6.1.6 but was PARP Ex. 6.1.6. OIG verified PARP Ex. 6.1.6 is PARP Ex. 6.1.6, and PARP Ex. 6 start date was PARP Ex. 6.1.6

OIG is providing this information and circumstances to your attention because of the sensitive position held by PARP Ex. 6.1.6. While OIG has not confirmed the information, we provide it to you to ensure that you address any alleged safety concerns. OIG encourages you and your staff to evaluate the information and take action as you deem appropriate. Should additional information be uncovered while deciding to take action, please contact me on PARP Ex. 6.1.6 or have a member of your staff contact Deputy Inspector General Rene Febles on PARP Ex. 6.1.6 or via email at PARP Ex. 6.1.6

M E M O R A N D U M

SUBJECT: Management Alert
PARP Ex. 6.1.6 Employee PARP Ex. 6.1.6
PARP Ex. 6.1.6

DATE: December 22, 2020

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding PARP Ex. 6.1.6. OIG's investigation into this matter is ongoing to determine if this information was identified during the background investigation and whether PARP Ex. 6.1.6 disclosed it during the interview process. OIG has alerted the PARP Ex. 6.1.6

OIG recently received two anonymous complaints concerning PARP Ex. 6.1.6. The complaints raised concerns that PARP Ex. 6.1.6. WMATA hired PARP Ex. 6.1.6 on PARP Ex. 6.1.6, and PARP Ex. reports to the PARP Ex. 6.1.6.

In PARP Ex. 6.1.6 2019, while PARP Ex. 6.1.6 was a PARP Ex. 6.1.6

OIG searched the PARP Ex. 6.1.6. Two cases related to the matter were identified in the PARP Ex. 6.1.6:

PARP Ex. 6.1.6

PARP Ex. 6.1.6

OIG is bringing these facts and circumstances to your attention because of the sensitive position held by PARP Ex. 6.1.6. Management should take action as deemed appropriate, even while OIG continues to investigate the matter. Should additional information be uncovered while you are deciding to take action, please contact me on PARP Ex. 6.1.6 or have a member of your staff contact Deputy Inspector General Rene Febles on PARP Ex. 6.1.6 or via email at PARP Ex. 6.1.6.

M E M O R A N D U M

SUBJECT: Management Assistance Report
Pension Plan Overpayments
(MAR-22-0001)

DATE: October 28, 2021

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) initiated a review of Washington Metropolitan Area Transit Authority's (WMATA) five retirement pension plans to determine whether improper payments were continuing after annuitants had died. The five pension plans are funded by payroll contributions from plan participants and by WMATA. OIG conducted interviews, gathered data, and engaged WMATA's Compensation and Benefits Office (CBO). As a result of our review, eight accounts from the Local 689 pension plan were identified as active accounts, when in fact the annuitant was deceased. Those eight active accounts should have been closed. CBO subsequently closed these accounts, and payments were discontinued in 2019.

Since February 2021, Local 689 legal counsel, through correspondence with the surviving family members, has engaged in reclamation efforts for the improper payments to individuals from these accounts in the amount of $440,219.

The results of the review indicated that WMATA did not have an internal mechanism in place to confirm continued eligibility of annuitants on an annual or recurring basis, or a method to ensure accuracy of the data within the active annuitant records. In addition, CBO does not maintain up to date annuitant records because it relies on an outside source, the annuitant fiduciary institutions (FI), to provide that data to CBO. Currently, CBO only tracks annuitants on Excel spreadsheets and not through an internal centralized electronic database.

The absence of defined roles, responsibilities, and internal controls has contributed to a lack of proper oversight and communication necessary to maintain accurate annuitant data. Another area of concern is the failure of Local 689 officials to provide requested annuitant data to WMATA's Accounting Office which interferes with proper oversight of pension plan funding and creates the potential for overpayments by WMATA. While this review focused

on decedent benefit payments, WMATA should improve its policies and procedures on the overall management of annuitant accounts.

CBO is the primary contact for retirees and communicates annuitant information to the FIs for the five pension plans. There are two FIs – one for Local 689 (Truist Bank - formerly SunTrust Bank), the largest pension plan, and one for Local 2, Local 922, Metro Transit Police Department (MTPD), and Non-represented employees (The Northern Trust Company). These FIs are responsible for facilitating payments to the annuitant either through an Automated ClearingHouse (ACH) deposit or the issuance of a check. The FIs are currently the only sources from which CBO obtains active annuitant account information across all five pension plans.

WMATA's Retirement Planning Manager is the primary contact with the FIs. The FI cannot make changes to the annuitant's account. CBO or the pensioner are the only ones that can update or change the status. In addition, the Transit Employees Health and Welfare Plan (TEHWP) may receive information on annuitant status.

It is important that all the stakeholders have a clear understanding of their responsibilities and that a defined process is in place to ensure timely communication. There needs to be assurance that updates and payments are adjusted or stopped as appropriate upon the death of an annuitant, and that there is a mechanism in place to confirm continued eligibility and accuracy of annuitant payments.

Originally CBO provided OIG with annuitant records for 8,037 "active" retiree accounts in Excel spreadsheet form. When OIG compared these records to Social Security Administration (SSA) death index data, 2,379 were reported as deceased according to SSA. OIG presented the findings of this analysis to CBO who, upon follow-up, advised OIG that they mistakenly had not purged these deceased annuitants (2,379) from the "active" records provided to OIG. Furthermore, CBO advised that the 2,379 retiree accounts were in fact properly closed upon the annuitant's death with no overpayments identified.

As a result of our review, OIG found that eight Local 689 pension plan annuitant accounts continued to make full annuity payments to surviving family members after the retiree died, even though the payments should have been stopped. The improper payments were stopped, and the accounts were closed once OIG identified the payments. The deaths of the eight annuitants occurred in the following years: 2015 (1), 2016 (2), 2017 (3), and 2018 (2). Overpayments to annuitants ranged from $6,700 to over $ 95,000. At the conclusion of the review, CBO confirmed overpayments to the eight accounts, which resulted in a loss to the Local 689 pension plan of $440,219. Based on WMATA's responsibility to contribute three percent annually to the Local 689 pension plan, WMATA's loss is approximately $13,206. Continued payments would have resulted in annual estimated losses to the pension plan of $220,990 and approximately $6,603 to WMATA.

Deceased Annuitant Overpayment / Loss Totals – Stopped April 1, 2019

ANNUITANT	DATE OF DEATH	LOSS
PARP Ex. 6.1.6		$95,086.66
		$29,244.70
		$82,842.87
		$41,269.57
		$6,712.39
		$8,769.85

Deceased Annuitant Overpayment / Loss Totals – Stopped August 1, 2019

ANNUITANT	DATE OF DEATH	LOSS
PARP Ex. 6.1.6		$80,515.94
		$95,778.05

TOTAL LOSS*	$440,219.86

**Gross Loss due to State or Federal taxes, according to WMATA's Benefits office.*

Amount Saved One Year from Termination of Annuity Payments

ANNUITANT	GROSS FINAL PAYMENT	X 12 MONTHS (SAVINGS)
PARP Ex. 6.1.6	$2,138.41	$25,660.92
	$1,499.49	$17,993.88
	$3,042.27	$36,507.24
	$2,226.33	$26,715.96
	$1,306.14	$15,673.68
	$1,466.60	$17,599.2
	$2,296.49	$27,557.88
	$4,440.11	$53,281.32

TOTAL SAVINGS	$220,990.08

OIG identified areas that need improvement to maintain an accurate accounting of eligible annuitants in CBO annuitant records, ensure proper record keeping and payment to annuitants, and develop a defined workflow process among all stakeholders for managing annuitant accounts. WMATA should develop an electronic database similar to PeopleSoft or a subset of PeopleSoft to manage retiree data and annuitants. CBO should maintain an up to date, internal database on active retiree annuitant accounts and not rely on the FIs for this data.

In April 2021, OIG obtained the "current" data on active retirees who were issued Retiree OneBadges (access to bus and rail badges) from the Office of Badging and Credentialing (OBC), which is under the Office of Security and Infrastructure Protection, MTPD. As a

result, OIG received in Excel spreadsheet form a list of 5,901 "active" retirees with a corresponding OneBadge issued to them. However, during a random sampling of the first 100 retirees on this list, seven were identified through open source data as being deceased. When OIG followed up, OBC acknowledged that the spreadsheet was not up to date and advised that there was currently no mechanism in place to regularly check the continued eligibility status of retirees with issued badges.

To better define roles and responsibilities within the process, OIG recommends that WMATA develop consistent standards and processes to ensure: (1) reliable data matching with both internal and external stakeholders; (2) confirmation, on a recurring basis, of the living status of annuitants either through SSA death index data checks or through commercially available data sources; and 3) timely notifications and updates of an annuitant's death to the paying FIs, the pension plan officers, health care providers, TEHWP, and WMATA's Badge and Credentialing Office. CBO should also notify the Office of Accounting when an annuitant dies. This would help ensure that WMATA's contributions to the plans are accurate and mitigate erroneous payments to the plans as well.

OIG is encouraged by the actions being taken by CBO to ensure that future overpayments do not occur, and notifications of an annuitant's death are identified and received timely. In June 2021, CBO advised OIG that steps had been taken to ensure future improper payments do not occur. A "Death Audit Report" will be run through the SSA on a quarterly basis. The FIs will notify CBO when informed of an annuitant's death, and a formal communication agreement has been established between CBO and TEHWP to make monthly reports of annuitant deaths.

However, it is critical that CBO have formal written policies, procedures, and internal controls in place to confirm the eligible status of annuitants. In addition, these internal controls should ensure that payments are stopped or reduced to survivor benefit levels, deceased annuitants are purged from the active records, and that all stakeholders are notified of an annuitant's change in status. By taking these actions, WMATA will ensure that the pension plan funds are being properly administered and protected.

We recommend the General Manager/Chief Executive Officer take the following actions to address the issues identified above and apply these controls to the other pension funds to mitigate erroneous payment contributions made by WMATA for all pension funds:

1. Establish a centralized automated database that will serve as a single source of truth to track retiree data and benefits for all stakeholders that manage aspects of retiree benefits, i.e. CBO, Accounting and MTPD.

2. Establish written policies and procedures for all WMATA stakeholders to enhance collaboration and consistent process in managing the various aspects of retiree benefits including validating WMATA's contribution payments to the union for pensions and validating the badging and credentialing for authorized retirees.

3. Formalize an agreement between WMATA and SSA to obtain SSA quarterly Death Index which allow for quarterly matching to validate WMATA records of retirees.

4. Establish formal sharing agreements with the union pension trustees to obtain retiree data on a regular basis to allow for matching against WMATA, FI, and SSA data as part of an ongoing data validation process.

5. Establish an annual certification process to validate active annuitant records and identify deceased or inactive retiree accounts.

6. Establish a process to certify the accuracy of annuitant data to be used by WMATA's Office of Accounting to mitigate erroneous payment contributions to union pension funds.

In addition to this Management Assistance Report, the Office of Investigations has also issued a Report of Investigation.

M E M O R A N D U M

SUBJECT: Management Alert (MA-22-0001)

DATE: November 5, 2021

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding the integrity of the procurement process for a federally-funded contract, PARP Ex. 6.1.4. OIG has obtained and verified evidence that multiple vendors who submitted bids for consideration on this contract were provided insider information and internal WMATA solicitation documents before the public release of the solicitation.

OIG received information that an inquiry was made from an associate of vendor, PARP Ex. 6.1.4, regarding the solicitation for PARP Ex. 6.1.4, which had not yet been publicly released. OIG determined PARP Ex. 6.1.4 had been approached by another vendor, PARP Ex. 6.1.4, who was in possession of internal WMATA solicitation documents, to include the unreleased scope of work (SOW). According to PARP Ex. 6.1.4 was seeking PARP Ex. 6.1.4 partnership in bidding for the contract because PARP Ex. 6.1.4 did not have the independent capacity to provide the requested PARP Ex. 6.1.4.

When interviewed by OIG, PARP Ex. 6.1.4 confirmed they sought partnership with PARP Ex. 6.1.4 for this contract and received internal WMATA solicitation documents. The PARP Ex. 6.1.4 owner stated PARP Ex. had been contacted telephonically by an unknown individual claiming to have insider information on the contract. The PARP Ex. 6.1.4 owner ultimately received hardcopy internal WMATA solicitation documents, including the SOW, from this individual during a subsequent in-person meeting in exchange for PARP Ex. 6 commitment to hire the individual as a subcontractor upon contract award. The PARP Ex. 6.1.4 owner did not have sufficient information to conclusively identify the source of the non-public WMATA solicitation documentation. OIG's investigation into the identity of this individual is ongoing.

The PARP Ex. 6.1.4 owner, who had little capability to independently provide the requested PARP Ex. 6.1.4, subsequently shared this non-public solicitation documentation with in an attempt to develop a joint bid for the contract. PARP Ex. 6.1.4 confirmed this account of events and provided evidence of the documentation they received from PARP Ex. 6.1.4, explaining

this is what led to PARP Ex. 6.1.4 solicitation inquiry with the PRMT official in PARP Ex. 6.1.6 2021. PARP Ex. 6.1.6 and PARP Ex. 6.1.4 ultimately submitted separate bids for PARP Ex. 6.1.4.

On PARP Ex. 6.1.6 2021, OIG met with PARP Ex. 6.1.6 and PARP Ex. 6.1.6 to discuss the compromised solicitation process. During this meeting PRMT explained, unbeknownst to OIG, that the contract PARP Ex. 6.1.4 awarded to PARP Ex. 6.1.4. According to PRMT, PARP Ex. 6.1.4 PARP Ex. 6.1.4. PRMT notified OIG during this meeting that PARP Ex. 6.1.4 had been awarded the contract. Approximately three hours after OIG's meeting with PRMT, PARP Ex. 6.1.4 independently provided notice PARP Ex. 6.1.4

At this time, OIG cannot confirm how many other bidders on this solicitation, if any, also improperly received WMATA solicitation documents or pricing information prior to their bid submission. OIG continues to investigate the matter to determine if any other company may have received the information and from whom.

We are bringing these facts and circumstances to Management's attention for immediate action to ensure the integrity of the procurement process is maintained and to help safeguard WMATA's funds from improper use.

Should you need further information, please contact me at PARP Ex. 6.1.6. I am also requesting that you please provide OIG with any action taken by management response to this memorandum by PARP Ex. 6.1.6 2021.

cc: COUN – P. Lee
IBOP – J. Kuo
PRMT – S. Moore
MARC – E. Sullivan

M E M O R A N D U M

SUBJECT: Management Alert
Counterfeit Bus Parts (MA-22-0002)

DATE: April 5, 2022

FROM: OIG – Rene Febles

TO: GMGR – Paul J. Wiedefeld

The Office of Inspector General (OIG) is transmitting this Management Alert to elevate concerns regarding the integrity of bus parts purchased from the vendor, PARP Ex. 6.1.4 [redacted]. OIG has verified evidence that [redacted] has sold counterfeit goods to WMATA.

Background

In 2016, WMATA posted a public solicitation for additional inventory bus parts under WMATA solicitation number PARP Ex. 6.1.4. The solicitation was for bids on approximately [redacted] line item bus parts for WMATA's bus inventory. In addition to the other prerequisites, the written solicitation required all parts quoted in the bid indicate the manufacturer/brand name and part number.[1] PARP Ex. 6.1.4 vendors submitted a bid, to include PARP Ex. 6.1.4 submitted a bid for approximately [redacted] of the line items. [redacted] listed PARP Ex. 6.1.4 as the manufacturer for all line items in their bid, along with the PARP Ex. 6.1.4 part numbers associated with each line item in their bid PARP Ex. 6.1.4 [redacted] was a WMATA-approved brand name for these parts).

PARP Ex. 6.1.4 was deemed to be the lowest bidder for approximately [redacted] of the line items submitted. As a result, in [redacted] of 2017, [redacted] was awarded a PARP Ex. 6.1.4 [redacted] contract to supply those PARP Ex. 6.1.4 line items for WMATA's bus inventory needs. WMATA exercised option years for this contract and entered into modifications, increasing the contract value to over PARP Ex. 6.1.4. Since 2017, WMATA has paid [redacted] more than [redacted] under this contract.

In addition to this contract, [redacted] has sold items to WMATA through a series of smaller contracts, dating back to [redacted], as well as through purchases made by WMATA Purchase Cards.

[1] If the vendor proposed an alternate part, they had to provide proof that the product complied with industry standards, to include analysis reports from an accredited independent laboratory.

Investigation

OIG received an allegation through our hotline that indicated [redacted] was selling counterfeit products to WMATA, to include PARP Ex. 6.1.4. OIG initiated an investigation into this allegation. As part of this investigation, OIG uncovered Material Discrepancy Reports (MDR) from WMATA Supply Chain Management receiving inspectors who conducted a quality inspection on ten of the PARP Ex. 6.1.4 sold to WMATA by [redacted]. These [redacted] were sold to WMATA as being PARP Ex. 6.1.4, PARP Ex. 6.1.5 [redacted]

In PARP Ex. 6.1.6 of 2020, WMATA purchased and received from [redacted] a shipment of PARP Ex. 6.1.4 [redacted] As part of their investigation, OIG had a team of experts disassemble one of these PARP Ex. 6.1.4 to determine whether [redacted] sold WMATA counterfeit parts. The experts concluded that: the PARP Ex. 6.1.4 was not a "new" PARP Ex. 6.1.4 r; the PARP Ex. 6.1.4 was not a genuine PARP Ex. 6.1.4 remanufactured PARP Ex. 6.1.4 the presence of wear on the PARP Ex. 6.1.4 indicated it had been used for PARP Ex. 6.1.4 [redacted]; the PARP Ex. 6.1.4 had been modified to make it look newer; and the PARP Ex. 6.1.4 contained inferior parts that were not genuine PARP Ex. 6.1.4 parts.

The OIG investigation is currently ongoing. The allegation of counterfeit parts was not limited to PARP Ex. 6.1.4. At this time, OIG cannot confirm how many other items received from [redacted] have been counterfeit goods of inferior quality. OIG is bringing these facts and circumstances to Management's attention for immediate action to ensure the integrity of WMATA's inventory and to ensure the safety and reliability of WMATA's Bus fleet.

At this time, OIG requests that you limit the sharing of this information to only those individuals who will aid in determining any information needed to fully assess the matter. As always, OIG is willing to assist in any way necessary.

cc: COUN – P. Lee
COO – J. Leader