MEMORANDUM

SUBJECT: Management Assistance Report
OIG Concerns Over Critical Cybersecurity
Vulnerabilities That Remain Unresolved
(MAR-23-0003)

DATE: February 17, 2023

FROM: OIG – Rene Febles [redacted]

TO: GM/CEO – Randy Clarke

The Office of Inspector General (OIG) is transmitting this Management Assistance Report (MAR) based on an ongoing cyber investigation initiated by our office regarding allegations of a data security breach or leak.[1] The incident initially giving rise to OIG's investigation occurred in early January 2023. OIG briefed the Board of Directors and the GM/CEO about that incident and related matters on January 26, 2023.

As OIG continues to investigate the January incident, several other matters relating to cyber weaknesses and vulnerabilities in WMATA operations have come to OIG's attention or have taken on heightened urgency. The most immediately concerning of these are summarized below. These matters, in the aggregate, are a cause for grave concern that WMATA's data, networks, and assets are at unacceptable risk of malicious penetration and compromise.

During OIG's investigation, evidence has surfaced that WMATA, at all levels, has failed to follow its own data handling policies and procedures as well as other policies and procedures establishing minimum levels of protection for handling and transmitting various types of data collected by WMATA. WMATA also lacks visibility into remote user activity, leaving it blind to the transfer of critical/sensitive data to devices outside of WMATA's control. OIG has found evidence of critical/sensitive data in devices outside WMATA's control containing network passwords, emergency response procedures, disaster recovery measures, vulnerability assessments, application/server diagrams and other critical/sensitive data.

Furthermore, WMATA has failed to implement at least 51 IT and cyber security recommendations intended to protect WMATA's data, networks, and assets. Some of these unimplemented recommendations date back to 2019. At least three commissioned outside

[1] Washington Metropolitan Area Transit Authority (WMATA) policy instruction 15.12/2, *Data Sensitivity*, defines a data security breach or leak as, "An incident of unauthorized access to, and acquisition of unencrypted or un-redacted records or data containing sensitive information."

~~"This document contains sensitive information and is the property of the WMATA Office of Inspector General (OIG). It should not be copied or reproduced without the written consent of the OIG. This document is for OFFICIAL USE ONLY, and its disclosure to unauthorized persons is prohibited in accordance with WMATA P/I 7.8.10/5 – Code of Ethics, Section 5.07. It must be protected during transmission, handling and storage in accordance with WMATA P/I 15.12/2 – Data Sensitivity."~~

cybersecurity-related reports as well as OIG and internal audits of WMATA's cybersecurity vulnerabilities have highlighted how, for years, WMATA has failed in its Information Technology (IT) responsibilities by not implementing basic IT policy changes and an IT governance framework focused on protecting WMATA's critical/sensitive data, networks and assets.

WMATA's long-standing failure has likely limited its ability to mitigate vulnerabilities. [redacted]

Although OIG's cyber investigation is still ongoing, OIG was compelled to issue this Management Assistance Report now in order to elevate to WMATA's Executive Leadership the multitude of IT-related critical recommendations, policy violations, and unsound IT practices that continue to plague WMATA. In order to mitigate the continued risk of loss or compromise of critical/sensitive data, WMATA must immediately establish security controls for restricting access to its data at all levels. These security controls include, but are not limited to, identity and access management, data loss prevention, encryption, and policy management and enforcement. Lack of immediate action on the part of WMATA leadership will leave WMATA susceptible to continued compromise of its critical/sensitive data, networks, and assets.

Background

OIG's cyber investigation was initiated after the OIG was alerted by WMATA's cyber security group in early January 2023 that it had detected abnormal network activity originating in Russia. WMATA's initial findings showed that the credentials of a contractor who was no longer working for WMATA had been used to access a sensitive WMATA directory from Russia. WMATA's initial assessment attributed the incident to a possible [redacted] WMATA confirmed that the contract had expired, and the contractor did not work for WMATA at the time of this incident. His WMATA supervisor, however, had allowed the contractor to retain his high-level administrative access to WMATA systems and networks, hoping the contract would be renewed. OIG's investigation, however, revealed that the former contractor's initial version of events was not truthful. The computer in Russia was turned on at the direction of the former contractor who remotely accessed his computer in Russia. Since the former contractor's high-level administrative access had not been revoked, he was able to remotely access his personal computer in Russia to log into WMATA systems containing critical and sensitive WMATA data.

WMATA hired this contractor through a U.S. based company to work on sensitive WMATA applications and systems including WMATA's SmarTrip® application, which is used by WMATA customers to pay for fare at all Metrorail stations.

OIG also requested from WMATA a list of contractors supporting WMATA from outside the United States and was advised that the information requested was not tracked by WMATA.

Cybersecurity Risks of the [redacted] Train

In 2019, OIG raised to WMATA's attention concerns regarding possible cybersecurity vulnerabilities of the [redacted] train. At the time, WMATA was not conducting vulnerability assessments or penetration testing of system components. As a result of OIG's recommendations, in 2019, WMATA contracted a security company that conducted penetration testing in accordance with National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and Open Web Application Security Project (OWASP) Standards against the [redacted] train. The testing uncovered a number of actual cybersecurity vulnerabilities in the [redacted] train. At the time, the security company determined that the risk to WMATA's train in its current configuration was "critical."

The security company provided WMATA a written report of its findings. OIG was never provided a copy of the report until February 2023, despite our earlier requests. OIG has asked for an update on what has been done since 2019 to address the deficiencies identified in the report and was advised that WMATA would be ready to meet with OIG at the end of February 2023.

In addition to the WMATA commissioned report, two OIG recommendations about cybersecurity concerns relating to the [redacted] train are still open after WMATA has asked for multiple extensions, one of which would extend to mid-2024. OIG is concerned by the lack of urgency accorded to these deficiencies and the lack of transparency with OIG.

Lack of Encryption of WMATA Owned Mobile Devices

One of the primary security controls readily available for restricting access to WMATA's critical/sensitive information stored on mobile devices is encryption. WMATA Data Sensitivity Policy Instruction 15.12/2, dated 4/20/2018, states that sensitive information stored on any system or media that is subject to loss or theft (including laptops, Universal Serial Bus (USB) drives, diskettes, CD/DVDs, personal computers and departmental servers) must be encrypted whenever not in use. Systems susceptible to theft should be physically secured. In 2019, WMATA's internal audit and compliance group highlighted the increased risk that a stolen or lost laptop could lead to a breach of security and disclosure of business and customer information due to inadequate security controls. At the time, it recommended that WMATA should require all laptops in use throughout the organization to have full disk encryption installed. To date this recommendation remains unimplemented and WMATA's mobile devices are issued and deployed without encryption.

Lack of [redacted] Security Controls on Access [redacted]

The OIG investigation has identified vulnerabilities in WMATA's [redacted] access [redacted] controls. A subsequent review by a private entity contracted by WMATA identified security shortcomings and made recommendations to improve [redacted]. These recommendations included securing privileged access and credential theft mitigation as well as changes to WMATA’s current procedures impacting asset management, conditional access policies, data loss prevention and information rights management. OIG considers these to be critical recommendations requiring immediate attention and implementation.

IT Asset Management

The ability for WMATA, as a critical infrastructure entity, to manage IT assets is of fundamental importance. Poor asset management practices dramatically increase the chances that threat actors will be able to achieve their goal of stealing sensitive data or penetrating a network. Investigative activity has revealed that WMATA lacks controls or procedures restricting its assets from being transported outside the United States. WMATA also lacks controls or procedures limiting access to data systems or network systems from outside the United States. OIG learned through forensic and cyber reviews that a WMATA employee accessed data on WMATA’s network while on vacation abroad. Although the employee had the authority to access the data, OIG is concerned because it was done with personal devices using unknown wireless or cellular connections from a location outside the United States. OIG interviewed the employee who advised that he did this because he was never issued a WMATA computer. OIG does not currently know why he was not issued a WMATA computer. Using personal devices increases WMATA’s risk of compromise.

WMATA Policy/Instruction 15.4, *Network Infrastructure Policy*, allows, but specifies requirements and limitations on, the use of personal electronic devices to access WMATA’s network and data. Those requirements and limitations have not been followed or enforced, however. This policy at present remains in force. After OIG questioned this and other policies, WMATA immediately revised a separate policy, Policy/Instruction 15.3/5, *Electronic Access Usage Policy*, to prohibit the use of personally owned devices as a general rule. As of January 25, 2023, P/I 15.3/5 prohibits the access or transmission of any WMATA information on a personal device or other non-WMATA issued device unless expressly authorized by a valid contract approved by Information Technology Security, or by the Senior Director, Cybersecurity. Thus, there is now an apparent conflict between Policy/Instructions 15.4 and 15.3/5. OIG plans to verify which, if either, policy is being applied and enforced. Additionally, WMATA currently does not know how many contractors and employees used, or still use, a personal computer for WMATA business or how WMATA will ensure that employees and contractors will comply with whichever policy applies.

Procurements Related to Cybersecurity

In 2020, WMATA awarded a contract to a company to provide human capital services associated with recruitment in various job categories. Even though the staff associated with this contract would be connecting to WMATA data systems and working from outside the United States, the initial contract was awarded without cybersecurity provisions or an assessment of how WMATA’s sensitive data would be accessed and protected. The cybersecurity team learned of this contract from WMATA employees who were concerned about the security implications. Once the cybersecurity team got involved, the team raised concerns about the access to be given the contractor. The cybersecurity team memorialized its concerns in a risk memo identifying all the risks the program office would be taking with this contract, but the program office never acknowledged or signed the risk memo prepared by the cybersecurity team. Ultimately the contract was executed, and the program office appeared to have overruled the cybersecurity team's concerns. Currently, OIG continues to assess how these contract employees are connecting to WMATA data systems from outside the United States, as it does not appear they have ever been issued WMATA owned devices. This issue will be the subject of a future OIG review.

<u>Unaddressed Vulnerabilities</u>

A global technology company recently analyzed WMATA's Vulnerability Management Program. In a 43-page report, the company stated that WMATA recognized its vulnerability risks, but that the organization had neglected its vulnerability to the point of never achieving a secure baseline. The report points out that WMATA has many resources already in place to aid its aspirations regarding basic cyber hygiene so it can achieve a sustainable environment. Success will be determined through management's support and commitment to facilitate the changes necessary to meet WMATA's goals in transitioning to a risk-based Vulnerability Management Program.

The report recommended that WMATA re-evaluate its [redacted]. Vulnerability management is commonly defined as the process by which an organization identifies, analyzes, and manages vulnerabilities in its critical services' operating environment(s).

Given the current threat environment, the report stated that it can be assumed vulnerabilities currently do or will exist within WMATA's systems. These vulnerabilities, if left unaddressed and subsequently become exploited by a threat, could render WMATA susceptible to unacceptable outcomes.

The consultant observed in its report that that there is a common theme of confusion in roles and responsibilities by WMATA staff related to vulnerability management procedures. In some cases, the tools available to accomplish the assigned responsibilities are not well understood. With this in mind, the report states that WMATA's executive management must pause to determine what its tactical goals are for the information technology and information security programs.

<u>Disconnect between IT Infrastructure and Cyber staff</u>

During interviews with staff, OIG learned that there is a disconnect between the IT infrastructure team and the cybersecurity team. The disconnect is so large that it has frustrated the cyber team, caused delays in implementation of important cybersecurity changes, and threatens WMATA's ability to protect its critical/sensitive data, networks, and assets.

We are aware that management is trying to make changes to address this environment. OIG has been advised that some of the infrastructure staff are part of Local Union 2, and that the union's collective bargaining agreement (CBA) has been cited as grounds to decline the implementation of various cybersecurity measures sought by the cyber staff. A CBA, should never interfere with essential functions that are needed for a robust cybersecurity program.

Corrective Action Plans and Other Reports

OIG's Audit and Evaluation reports provide recommendations to management at the completion of the audit or review. Once management responds to OIG with its commitment to take corrective action, those recommendations become individual Corrective Action Plans (CAPs). OIG tracks due dates for each CAP and provides the Board of Directors with a quarterly report on the status of each recommendation. WMATA also tracks all recommendations through its Audit and Compliance division.

In addition to OIG's work, Audit and Compliance, an internal WMATA Division, conducts audits and compliance reviews of WMATA Operations. Audit and Compliance was previously called Management Audits, Risk and Compliance (MARC).

In 2019, MARC conducted a "Cybersecurity Maturity Assessment and Information Security Follow-up Review," and issued its report on March 31, 2019. That report identified 64 findings of which 22 remain open. MARC identified six "High Risk" findings out of the 64. All six remain open today. OIG is concerned with the length of time these recommendations have remained open.

On February 9, 2023, OIG briefed the Board of Directors and the GM/CEO on the status of OIG recommendations. As of that date OIG continued to monitor 55 open recommendations. These open recommendations were initially presented to management between February 2019 and July 2022. Currently six open recommendations date back to 2019. These six pertain to cybersecurity and IT matters. OIG expressed concern about not only the age of these six open recommendations, but also the critical topics surrounding the recommendations. WMATA has requested multiple extensions on most of OIG's recommendations, with one requested extension extending to 2024.

OIG's Cybersecurity Audit

In 2022, OIG initiated an audit of WMATA's cybersecurity program. As a result of matters uncovered, OIG paused the audit to address those matters. In May 2022, OIG issued a Management Alert (MA) to the Acting General Manager and Chief Executive Officer (GM/CEO). On August 10, 2022, the IG provided the current GM/CEO the same MA expressing concern with issues in the report. As of the date of this report, OIG's concerns still stand. One of OIG's gravest concerns identified in the MA was access to WMATA data by foreign nationals who were supporting sensitive applications and systems from Russia.

WMATA outsources background investigations on individual contractors to the companies that employ them. OIG subpoenaed the company employing the foreign nationals to obtain the background investigations conducted on those contractors. Documents received revealed that 37 percent of the company's background investigations used the same last four digits of a social security number. As a result, OIG will be reviewing how WMATA handles background investigations.

OIG Recommendations

OIG recommends that the GM/CEO take the following action:

1- Immediately address all the concerns from OIG's May 2022 Management Alert with special emphasis on WMATA's Vulnerability Management Program (VPM) to include the concerns and recommendations contained in the independent analysis of WMATA's VPM.

2- Prioritize addressing all open CAP recommendations associated with IT or cybersecurity.

3- Establish a process to ensure WMATA's agreed upon CAPs are addressed with actual improvement changes and extensions are granted based on actual implementation progress.

4- Change the validation process for CAPS to ensure the agreed upon actions have been fully implemented.

5- Immediately address all issues associated with the 2019 [redacted] train penetration testing that exposed vulnerabilities.

6- Immediately address the recommendations made in the February 2023 Detection and Response Team assessment.

7- Identify and provide the OIG a listing of IT assets and devices that are connected to WMATA's network.

8- Provide OIG a list of all devices that have connected to WMATA's network or to Office 365 over the past 30 days to include the network connections' geolocation.

9- Immediately review and address contractor background security clearance concerns identified by OIG during its investigation.

10- Establish a process wherein WMATA can track, identify, and monitor the network activity of contractors supporting WMATA from outside the United States.

11- Establish a process in which all WMATA procurements include a cybersecurity assessment before they are awarded, and any risk is recognized and accepted by the EVP of the program office after discussion with the GM/CEO.

12- Thoroughly address the environment and problems between the IT infrastructure and cybersecurity staff giving cybersecurity concerns priority, particularly when the decisions degrade WMATA's ability to protect critical/sensitive data, networks, or critical assets.

13- Provide cybersecurity staff all authority to direct staff when it comes to cybersecurity concerns and make sure that their authority is communicated to WMATA personnel.

14- Immediately review and make changes as appropriate to all IT and cybersecurity policies to assure actual compliance and that they are suitable for the current cybersecurity threat environment as defined by the US Department of Transportation, the US Department of Homeland Security, and their respective critical infrastructure agencies.

This matter is being forwarded to you for review and action as appropriate. Please respond, in writing, by February 24, 2023, documenting any actions planned or taken.

cc: WMATA Board of Directors
COUN – Lee

~~"This document contains sensitive information and is the property of the WMATA Office of Inspector General (OIG). It should not be copied or reproduced without the written consent of the OIG. This document is for OFFICIAL USE ONLY, and its disclosure to unauthorized persons is prohibited in accordance with WMATA P/I 7.8.10/5 – Code of Ethics, Section 5.07. It must be protected during transmission, handling and storage in accordance with WMATA P/I 15.12/2 – Data Sensitivity."~~

MEMORANDUM

metro

Washington
Metropolitan Area
Transit Authority

SUBJECT: Management Assistance Report: OIG Concerns Over Critical Cybersecurity Vulnerabilities that Remain Unresolved (MAR-23-0003)

DATE: February 28, 2023

Torri Martin [redacted] WMATA

Digitally signed by Torri Martin [redacted] WMATA
Date: 2023.03.01 10:49:49 -05'00'

FROM: Chief Information Officer – Torri T. Martin
Chief Audit & Risk Officer – Elizabeth Sullivan (POC)

TO: OIG – Rene Febles

Thank you for the above-referenced management assistance report ("Report"). We have reviewed the report and appreciate the Office of Inspector General's ("OIG") assessment and recommendations regarding cybersecurity and certain business processes. We offer the following response to the Report.

The protection of the Authority's digital assets and sensitive data, while very important, must be balanced with the ability of the Authority to operate the Metro system. That said, the Authority's Information Technology ("IT") department has ongoing programs to implement cyber tools and other technologies to provide increased visibility, control, and enforcement capabilities of the Authority's IT network. The IT department also has implemented programs to integrate log data for enhanced alerting capabilities, as well as automation of responses in order to increase the effectiveness of the cyber program and response activities. The IT department has worked collaboratively with OIG and has periodically provided OIG with updates on these and other issues over the last several years. Since the beginning of 2023, the Office of Cybersecurity ("Cyber") has met weekly with OIG to discuss cybersecurity issues and share information.

Before addressing the matters raised in the Report, we respectfully note that the Report fails to recognize that the IT department has made measurable improvements in its cybersecurity program as demonstrated by successfully closing 142 out of 168 OIG corrective action plans ("CAPs") since 2019.[1] A few examples of significant cybersecurity improvement as a result of CAP closure include: (1) deployment of modern Managed Extended Detection and Response capabilities; (2) implementing an Incident Response program with reporting and documentation requirements; (3) selection and early adoption of the National

[1] The total number of CAPs closed include 7 that were consolidated into two other CAPs at the IT department's request to help improve efforts to address OIG's recommendations.

~~CRITICAL INFRASTRUCTURE SENSITIVE~~
~~BUSINESS PROPRIETARY AND CONFIDENTIAL~~

Institute of Standards and Technology ("NIST") Risk Management Framework, and (4) integration of cybersecurity requirements in the procurement process.

January 2023 Suspicious Activity

As a result of security and detection tools and technologies that have been implemented, the IT department was first to detect suspicious activity in the network in early January 2023 (referred to as a "data security breach or leak" in the Report). The suspicious activity was identified by Cyber using the User and Entity Behavioral Analytics tools and associated alerts that were deployed specifically to identify risky logons and to alert incident responders. As you know, the IT department proactively provided the incident alert and associated information to OIG. As we continue to investigate the incident, the IT department has retained and directed the Microsoft Detection and Response Team to perform a thorough investigation of the suspicious activity, identify indications of persistent malicious activity, and make recommendations to improve the overall cybersecurity posture of the Authority. The Microsoft team investigation produced three significant findings:

1. There was no concrete indication that the contents of the OneDrive were synchronized to the device in Russia.
2. No indications of persistence or ongoing malicious activity were observed.
3. The Microsoft team identified several opportunities to improve the cyber-resiliency of the Authority's IT network environment.

The IT department is currently evaluating the recommendations from the OIG's and the Microsoft team's respective assessments, which will inform how the recommendations will be prioritized, resourced, and aligned to existing programs as appropriate. Where a new program or process may be needed, we will develop an actionable plan and milestones based on available resources and appropriate CAPs.

[redacted] Rail Cars

The Authority was one of the first transit agencies in the country to perform a penetration test of rolling stock. Similar to rail car design practices at the time, the design requirements of the [redacted] did not include a specification that it be able to withstand common penetration testing techniques (a design requirement for that was added to the 8000 series procurement). The vulnerabilities identified in the penetration test were not known to the Authority, nor to the car builder and sub-suppliers. Importantly, while certain vulnerabilities were identified, at no time were the testers able to access or control any automatic train controls or operations.

Because the fixes for the penetration test vulnerabilities are new, the sub-suppliers are still developing the necessary software upgrades, while not adversely impacting overall rail car safety. The vendor estimates completion of the software upgrades by the [redacted]. Because the sub-suppliers are located around the globe, progress was severely impacted by the pandemic.

[redacted] The IT department and Operations are developing an integrated corrective plan for these efforts.

Concurrent with the above-mentioned efforts, the IT department is also addressing the two open recommendations from OIG's 2019 report on the security of the rail cars. Specifically, the IT department is developing: (1) an asset management program for all hardware and software within the rail car environment to manage the IT maturity of the rail cars as they age; and (2) a holistic, collaborative approach to identifying and mitigating cybersecurity risks in rail cars that is based on recognized governance frameworks such as the NIST Cybersecurity Framework. The actions are targeted for completion on or about [redacted].

Metro-owned Mobile Devices and [redacted] Access Controls

The IT department is utilizing Zero Trust Architecture ("ZTA") principles to modernize and improve the security of WMATA's digital assets and data. ZTA is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital

~~This document contains **CRITICAL INFRASTRUCTURE SENSITIVE** information and is the property of Washington Metropolitan Area Transit Authority. It should not be copied or reproduced without the written consent of WMATA. This document is for **OFFICIAL USE ONLY** and its disclosures to unauthorized persons is prohibited in accordance with WMATA P/I 7.8.10/5 – Code of Ethics, Section 5.07. It must be protected during transmission, handling, and storage in accordance with WMATA P/I 15.12/2 – Data Sensitivity.~~

interaction. This strategic approach has two key elements: strong device compliance and strong identity management. For device compliance, the IT department will utilize mobile device management tools to maintain and enforce compliance with device encryption, patch status, and secure configuration. This effort is targeted for operational status by [redacted], with continuous improvement thereafter. For identity management, the IT department has an existing capital project designed to implement many high priority access controls, including [redacted]. This program will strengthen access controls pending program completion on or about [redacted].

IT Asset Management

The IT department utilizes many sources of data to identify digital assets, including inventory applications, active directory, vulnerability scanning tools, network management tools, and other cybersecurity tools. The next step is to integrate these data sources into a single tool, which will serve as a Configuration Management Database ("CMDB"), providing a single authoritative source for identifying the physical and virtual location of an asset, as well as its ownership and defined use/role. The IT department has selected an industry leading CMDB tool and is currently in the process of populating the data. We are striving to have the data populated and the program operational on or about [redacted].

Various Assessments and Reviews

In addition to the specific information outlined above, many of the matters raised in the Report had already been identified by prior Authority initiated assessments. The IT department is already working to address process gaps and minimize network vulnerabilities identified in these prior assessments. As part of our ongoing process of reviewing and hardening our IT network, we will continue to incorporate the OIG's recommendations as appropriate. We note that many of the corrective actions and programs already implemented by the IT department as well as those that address most of the recommendations in the Report will require multiyear efforts and significant capital investments. For example, the capital project designed to implement many of the high priority access controls over the Authority's data and systems is currently projected to cost $15.8 million over three years.

We note further that while the Report identifies the existence of vulnerabilities, the Report does not analyze the likelihood of those vulnerabilities being exploited nor does it identify the potential business impact. The IT department in coordination with other departments are in fact analyzing the risks and probability of vulnerabilities and prioritizing resources and corrective actions accordingly. For example, Cyber's Threat Hunt Team has performed 14 penetration tests of various systems during fiscal year 2023 to identify exploitable vulnerabilities and test the Authority's security posture. To date, these aggressive simulations of common threats and trend scenarios utilizing known vulnerabilities indicate that the Authority's overall cyber risk is low. The 14 penetration tests were conducted on high priority systems including our [redacted]

Finally, we note that the IT department has already submitted information and sought closure of all the CAPs associated with the OIG's May 2022 Management Alert. The IT department is currently preparing responses to follow-up requests from the OIG and the Audit & Compliance department to complete these corrective actions.

Next Steps

In addition to the actions and programs described above that will address the matters raised in the Report, the IT department will also do the following:

1. Develop CAPs to address the issues identified by the Microsoft team.

2. The IT department will prepare a crosswalk of all recommendations from IT assessments from 2019 to date to map recommendations, identify and group duplicates, and associate recommendations to relevant CAPs. This crosswalk is expected to be completed on or about [redacted].

3. The IT department will work with the Procurement department to determine whether the contractor complied with its background check requirements and submitted *bona fide* quarterly background check certifications as required in its contract with the Authority.

4. Develop an integrated corrective action plan to address the hardware and software vulnerabilities identified for the [redacted] rail cars by [redacted].

~~This document contains **CRITICAL INFRASTRUCTURE SENSITIVE** information and is the property of Washington Metropolitan Area Transit Authority. It should not be copied or reproduced without the written consent of WMATA. This document is for **OFFICIAL USE ONLY** and its disclosures to unauthorized persons is prohibited in accordance with WMATA P/I 7.8.10/5 – Code of Ethics, Section 5.07. It must be protected during transmission, handling, and storage in accordance with WMATA P/I 15.12/2 – Data Sensitivity.~~

5. The comprehensive draft Cybersecurity Policy has been developed and pending review and approval by the new Chief Digital Officer. The final approved Cybersecurity Policy will be provided to OIG.

6. The IT department is reviewing the items requested in the Report, numbers 7 & 8, and is working to provide the information on or about March 31, 2023.

cc: Randy Clarke, GM & CEO

~~This document contains **CRITICAL INFRASTRUCTURE SENSITIVE** information and is the property of Washington Metropolitan Area Transit Authority. It should not be copied or reproduced without the written consent of WMATA. This document is for **OFFICIAL USE ONLY** and its disclosures to unauthorized persons is prohibited in accordance with WMATA P/I 7.8.10/5 – Code of Ethics, Section 5.07. It must be protected during transmission, handling, and storage in accordance with WMATA P/I 15.12/2 – Data Sensitivity.~~