M E M O R A N D U M

~~Security Sensitive Information // Critical Infrastructure Information~~

SUBJECT: WMATA Cybersecurity DATE: May 8, 2023

FROM: CISO – [redacted]

TO: TSA – [redacted] Assistant Administrator
TSA – [redacted] Deputy Assistant Administrator, Surface Operations

At the request of TSA, WMATA is pleased to provide this memorandum that sets forth (1) a timeline of a cybersecurity incident that occurred on January 4, 2023 (the "January 4 incident"), (2) a summary of immediate steps implemented to address the January 4 incident, and (3) a description of other actions taken or planned to harden WMATA's IT network. In WMATA's view, the January 4 incident was not a "breach" nor a "computer network attack" as those terms are defined by the National Institute of Standards and Technology ("NIST").

I. January 4 Incident

On 4 January 2023, WMATA's Office of Cybersecurity ("WMATA Cyber") received a cybersecurity tool alert – "Abnormal behavior: activity from new geolocation to the organization." The following information was in the alert:

- Username: [redacted] (Contr)
- [redacted]
- Geolocation of the activity: Russia

Washington Metropolitan Area Transit Authority

4 - 5 Jan: WMATA Cyber investigated the alert, including reviewing logs and contacting the reported user's on-site WMATA manager to establish context for the event. Initial investigation performed by WMATA Cyber led incident responders to believe that the activity was access synchronization activity.

5 Jan: WMATA Cyber coordinated with WMATA IT to block access to Office 365, disable administrator and normal accounts, and terminate active sessions.

6 Jan: WMATA Cyber notified WMATA OIG of the January 4 incident.

9 Jan: WMATA Cyber identified that [redacted] access had been re-enabled due to a business process error. WMATA IT terminated all

access again.

10 Jan: WMATA IT removed [redacted] from the [redacted] vendor contract and [redacted] was no longer permitted to work on WMATA matters.

10 Jan: WMATA OIG reported potential data transfer from [redacted] OneDrive to a computer in Russia (beyond normal access synchronization); WMATA OIG also reported inconsistencies in the statements made by [redacted] to both WMATA Cyber and WMATA OIG. It was subsequently determined that [redacted] was in the U.S. on January 4 at the time of the cybersecurity alert and [redacted] personal computer in Russia was the source of the alert.

12 Jan: WMATA Cyber began a review of data accessed by [redacted] that was now considered to be an active spillage. Based on this review, WMATA Cyber determined that [redacted] access to certain WMATA Active Directory accounts was consistent with [redacted] support of WMATA's [redacted] Web Applications.

18 Jan: WMATA Cyber reported the January 4 incident to U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"). The January 4 incident did not fit squarely into any of the four categories for mandatory reporting as described in TSA Security Directive-1582-21-01A. WMATA nonetheless voluntarily reported the incident to CISA out of an abundance of caution.

27 Feb: CISA closed WMATA's report of the January 4 incident without comment. *See* CISA [redacted].

II. January 4 Incident Response Remediation

25 Jan: WMATA IT changed passwords to accounts accessible by [redacted]

25 Jan: WMATA IT updated its Electronic Access Usage Policy (15.3/5), to authorize WMATA's Chief Information Security Officer ("CISO") to approve or deny remote VPN access to WMATA's IT network, accounts, and resources. WMATA IT will maintain a list of devices approved for access, which includes WMATA owned devices and non-WMATA devices that have been approved for use by WMATA's CISO (*e.g.,* with security provisions, anti-virus software etc.).

27 Jan: WMATA IT briefed the Board regarding the January 4 incident.

27 Jan – 10 Feb: WMATA brought in Microsoft's Detection and Response Team ("DART") to investigate and provide threat intelligence on the January 4 incident. DART found:

- There was no concrete indication the content of the OneDrive was synchronized to a device in Russia
- No indications of persistent or ongoing malicious activity were observed
- Identified opportunities (approximately sixty-three (63) unique recommendations) to improve the cyber-resilience of the environment

[redacted].

23 Feb – 28 Feb: Removed connectivity of four computers from the WMATA network based on the DART report and findings (the computers had RDP (Remote Desktop Protocol) exposed to the public).

27 Feb: WMATA Cyber implemented a file classification scan [redacted] of all files contained in [redacted] OneDrive to identify all data types, which confirmed that there was no personally identifiable information (e.g., social security numbers) and no payment card data.

III. Ongoing and Planned Actions to Harden WMATA's Network

This section summarizes ongoing and planned actions to harden WMATA's network and improve cyber resiliency. We note that WMATA's new Chief Digital Officer, who will report directly to WMATA's General Manager and Chief Executive Officer, will join WMATA in May 2023 [redacted]. In light of this, we anticipate that the new Chief Digital Officer will develop a comprehensive IT strategy which may further refine, supplement, or modify the actions noted below.

WMATA continues to prioritize the security of our data, systems, and network. Our Cyber Fusion Center will enhance and improve our enterprise cybersecurity. WMATA IT's cybersecurity services, which includes threat detection and response, analytics, and advance security tools, will enable us better integrate security activities and reduce risks across WMATA.

A. [redacted]

[redacted] was a contractor with [redacted] a WMATA vendor. As of September 30, 2022, WMATA required and confirmed that any [redacted] employee working on WMATA matters must do so only from within the United States.

WMATA has another existing vendor, [redacted] who will provide the web application support currently provided by [redacted] At WMATA's direction and coordination, [redacted] is currently winding-down its work on WMATA matters and in the process of transitioning all work to [redacted] The [redacted] contract will expire on June 30, 2023.

B. WMATA IT Network Changes and Remediation:

As of April 14, WMATA IT migrated all servers and systems from WMATA's onsite data center to [redacted] a third-party data center, and is in the process of migrating the Web Applications supported by [redacted] to the Microsoft Azure cloud. As a result, all IP addresses, IT network diagrams, and technical architecture have been changed, and therefore [redacted] access and knowledge of these components are now obsolete.

WMATA Cyber intends to implement each of the DART recommendations. WMATA's General Manager and Chief Executive Officer has committed to funding this capital project. In the meantime, WMATA IT has already executed two of the most critical findings: (1) [redacted], and (2) [redacted].

[redacted]

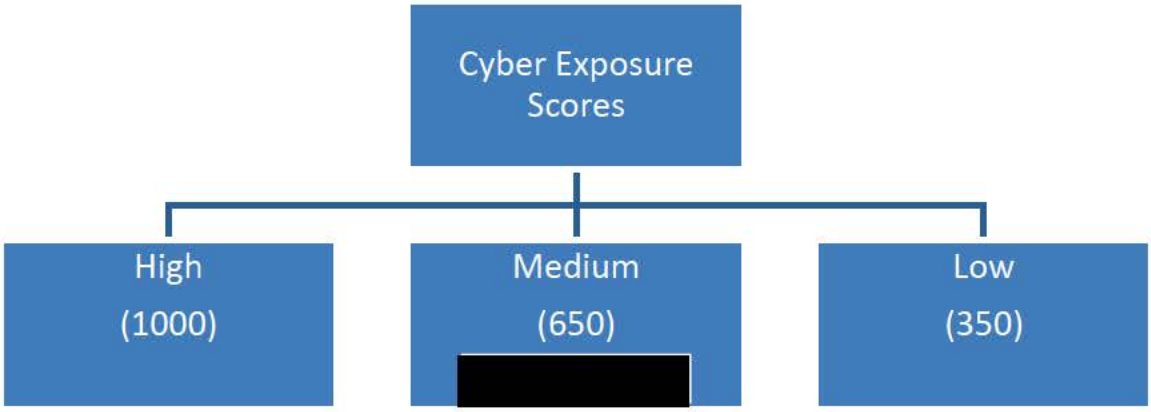
C. Actions to Remediate Vulnerabilities:

WMATA Cyber uses [redacted] tool to identify vulnerabilities. We note that understanding how vulnerabilities are measured is necessary to evaluate the import and meaning of the "number" of vulnerabilities. The number of vulnerabilities may vary widely due to different terminologies, the type of reporting queried, the number of assets in scope, or the dashboard used. WMATA Cyber queries and customarily reports on the number of individual patches applied

(Common Vulnerabilities and Exposures (CVEs) remediated) and the number of vulnerabilities remediated. The number of vulnerabilities fluctuate daily, thus a trend over time is a more meaningful metric. At present, [redacted] reports [redacted] **vulnerabilities** across all assets down from [redacted] vulnerabilities reported in June 2022.

Another significant metric is the [redacted] Cyber Exposure Score (CES). The CES is a useful and important roll-up of data across all recent scans, the aggregate asset exposure, and other factors that impact the true vulnerability of assets [redacted]

WMATA's CES is currently [redacted], down from [redacted] in June 2022. WMATA IT aims to have our CES below 350 by the end of the summer, with continual program improvement thereafter. Consistent with industry standards, it is important to note that there will always be vulnerabilities present on WMATA digital assets. No program can achieve 100% remediation.



The significant decrease in WMATA's CES score may be attributed to WMATA's interim TIGER team (internal subject matter experts from across WMATA IT) that was formed in June 2022 to prioritize patching vulnerabilities until a permanent TIGER team is established.

The permanent TIGER team reporting to WMATA's Chief Technology Officer (CTO) will be responsible for patching any inadequately supported servers on the network. We anticipate that the TIGER team will include four system administrators to install patches and a program coordinator responsible for managing reports, prioritizing remediation, and updating senior management on the progress of

WMATA's Vulnerability and Patch Management Program.

D. Network Access Management:

Consistent with the updated Electronic Access Usage Policy, WMATA IT is developing a technical methodology to fully implement this policy change. WMATA IT is seeking to leverage [redacted] to control access from non-WMATA devices. We expect to have this implemented in early 2024. In addition, WMATA IT is formalizing the processes and procedures to implement the policy.

E. Submission and Approvals by TSA:

As you know, pursuant to TSA Security Directive-1582-21-01A all covered agencies are required to submit to the TSA a Cybersecurity Incident Response Plan and to conduct a cybersecurity vulnerability assessment and submit the assessment results form to TSA. WMATA has completed both tasks.

On April 21, 2023, WMATA Cyber submitted its Cybersecurity Incident Response Plan to TSA. TSA reviewed the plan (November 9, 2022) and determined that the plan was compliant (March 2, 2023).

In March 2022, WMATA conducted a cybersecurity vulnerability assessment as required by TSA Security Directive-1582-21-01A. On March 22, 2022, WMATA submitted the results of the assessment to TSA and TSA determined that the assessment complied with TSA's directive.

Finally, TSA has offered some of its cybersecurity services, such as 5N5 Workshop and Validated Architecture Design Review, to help WMATA strengthen its cybersecurity environment. WMATA intends to avail itself of TSA's services. WMATA's CISO has been in contact with TSA's [redacted], Cyber Director, Surface Operations, and they currently plan to meet in person at WMATA's headquarters the week of May 15.

[redacted]

cc: GM & CEO – Randy Clarke