GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

OIG

CONFIDENTIAL

February 24, 2023

The Honorable Muriel Bowser
Mayor of the District of Columbia
District of Columbia
The John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 316
Washington, D.C. 20004

Kevin Donahue
City Administrator
Office of the City Administrator
The John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 521
Washington, D.C. 20004

Re: **Management Implication Report (MIR)**[1] – Cybersecurity Management Practices

Dear Mayor Bowser and City Administrator Donahue:

In accordance with D.C. Code § 1-301.115a(a-1)(3), which requires me to inform District leadership of issues related to the administration of government programs and operations, I am sending this MIR to notify you of potential cybersecurity risks that may negatively impact the District's ability to conduct operations.

Background

According to the *Internet Crime Report* issued by the Federal Bureau of Investigation (FBI),[2] the cost of cybercrime in the United States totaled $6.9 billion in 2021. While private businesses and financial institutions remain the primary target of cybercrimes, governments remain a target due to the potential to monetize the abundant personal information within federal, state, and local databases. In recent years, District agencies have experienced cyberattacks that have impacted operations, led to the loss of critical information resulting in material weaknesses in audit findings, and have suffered direct financial loss.

[1] The OIG issues Management Implication Reports (MIRs) to inform multiple District agencies of a matter that surfaced during the OIG's oversight work. MIRs are publicly available on the OIG website.
[2] U.S. DEP'T OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME REPORT 2021 at 7, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (last visited Feb. 9, 2023).

Since 2021, two District agencies have been the victim of ransomware attacks where sensitive information was compromised, which impacted District operations. In one incident, personal data was stolen and subsequently posted to the Dark Web. In a second incident, agency financial data was stolen, impacting the agency's ability to accurately

provide financial statements for annual audit. A failure to strengthen IT-related controls can create conditions in which the District risks material misstatements of its financial reporting that can adversely impact the District's financial reputation.

These two incidents bring into sharp focus cybersecurity-related IT risk(s) that may exist within the District government, including independent District entities – some of which may fall outside the direct oversight and authority of the Office of the Chief Technology Officer (OCTO).[3] Due to increasing reliance on information technology to perform government operations, the District must be aware of potential cybersecurity threats and ensure that all agencies have effective IT-related internal controls, including a Cyber Incident Response Plan to mitigate the damage of a cyber-attack.

Cybersecurity Threats

As methods used to conduct cybercrimes are constantly evolving, the District must ensure that processes and procedures are in place to prevent/mitigate these threats. According to leading cybersecurity organizations, the following are some of the most concerning threats facing organizations in 2023:

- **Business Email Compromise (BEC) and Phishing**. BEC remains a primary cybersecurity threat and can facilitate other schemes. BEC scams exploit our reliance on email to conduct personal and professional business. In these schemes, a scammer may use phishing tactics, such as sending emails or other messages purporting to be from reputable companies from spoofed email accounts or websites of legitimate organizations, to get an employee to unwittingly send confidential information, change vendor information to cause an improper payment, or install malware to give the scammer access to the victim's system. While traditional phishing emails, such as the notorious Nigerian prince scam, may have been easy to spot, scammers are now more sophisticated, and avoiding these scams has become more difficult. Cybersecurity and phishing awareness training remain critical in addressing these types of threats.

- **Ransomware and Malware**. As the use of ransomware and malware increases, the costs to an organization, in terms of financial loss and the amount of stolen data due to these attacks, continue to rise. In these schemes, attackers gain access to an organization's systems and install malware or ransomware to either download confidential data from the system or encrypt data on the host system so the organization cannot access it. In the case of ransomware, after gaining access to the organization's system and data, the attacker will contact the victim and request payment in exchange for decrypting the data. Increasingly, as organizations refuse to pay ransoms, attackers are beginning to remove data from the system instead of, or while simultaneously encrypting the system data and threatening the public release of the information when victims refuse to pay. However,

[3] D.C. Code § 1-1402.

because the primary goal is to encrypt data to obtain a ransom in exchange for decrypting the data, even when a decrypter is provided after payment, it may not work. The ransomware threat has increased with the proliferation of Ransomware as a Service (RaaS) providers, such as the recently disrupted group Hive,[4] that enable smaller organizations and individuals to use sophisticated, already-developed ransomware tools to execute attacks against a wider variety of targets.

- **Zero-day attacks.** During a zero-day attack, a hacker exploits a hardware or software system vulnerability before a developer can identify and patch it. While zero-day attacks targeting websites or software applications remain a threat, zero-day attacks against edge devices are a growing threat. Edge devices are the hardware that controls data flow at the boundary between two networks. Examples of edge devices include edge routers, routing switches, firewalls, and other wide area network (WAN) devices. Bad actors can use these devices' vulnerabilities to gain network access covertly. Therefore, organizations should regularly evaluate their systems and devices for vulnerabilities and immediately patch them. Patching vulnerabilities is critical for older IT systems as outdated software and equipment may not receive regular security updates for evolving cyber threats, such as ransomware. OCTO maintains a cybersecurity waiver system that provides District government agencies extended time to fix identified vulnerabilities. While there may be legitimate situations in which these waivers are necessary, delays in patching vulnerabilities may leave the District susceptible to zero-day attacks. Organizations should address identified vulnerabilities as soon as possible.

Cyber Incident Response Plan

Cybersecurity awareness programs for employees are critical to avoid phishing and BEC schemes. However, organizations must also have a plan in place for dealing with the more sophisticated attacks and breaches when they occur. OCTO has published policies addressing an effective response plan that apply to every agency connected to the District network;[5] however, agencies independent of OCTO must also ensure they implement a plan. The National Institute of Standards and Technology (NIST) published a *Computer Security Incident Handling Guide*[6] to help organizations develop an effective response plan. NIST identifies four phases to handling an incident: (1) preparation; (2) detection and analysis; (3) containment, eradication, and recovery; and (4) post-incident activity.[7]

Preparation - An organization must determine how to respond to an incident before an attack happens. According to industry standards, an organization must have the following:

[4] Press Release, U.S. Dep't of Justice, Office of Public Affairs, U.S. Department of Justice Disrupts Hive Ransomware Variant (Jan. 26, 2023), https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (last visited Feb. 9, 2023).
[5] D.C. Office of the Chief Technology Officer, Cyber security Incident Response Team Policy, (revised May 25, 2021), https://octo.dc.gov/node/1523591 (last visited Feb. 15, 2023).
[6] U.S. Dep't of Commerce, National Institute of Standards and Technology, Computer Security Incident Handling Guide (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (last visited Feb. 9, 2023).
[7] *Id.* § 3.

- **Cyber Incident Response Team.** As part of their plan, organizations should establish a Cyber Incident Response Team and identify members, their roles and responsibilities, and what authorities they have in the event of an incident. There are different ways to structure a response team, but agencies need to identify the structure, resources available, and internal and external dependencies for the team. When formulating the team, agencies need to consider that responding to a cyber event often involves interacting with third-party vendors, the media, and law enforcement.

- **Cybersecurity Risk Assessment.** As detailed in the OCTO Risk Assessment Policy,[8] all organizations "must conduct assessments of the risks, including the likelihood and magnitude of the harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits." Organizations should regularly monitor and scan for vulnerabilities in their systems, employ vulnerability monitoring tools and techniques, and remedy vulnerabilities as soon as possible in accordance with the District's Vulnerability Management Policy.[9] Delays in identifying and patching vulnerabilities leave hackers with an avenue to infiltrate and attack a system. As detailed in the District's FY 2022 Annual Comprehensive Financial Report (ACFR), failure to perform vulnerability scanning on a routine basis contributed to a recent District cyber incident.

- **Data Disaster Recovery Plan.** As the threat of ransomware and data extortion increases, it is crucial that agencies back up their data regularly and, just as importantly, test their backups to ensure systems and data can be restored when needed. Cybersecurity companies report that clients often fail to test their data backup and recovery process only to find that it does not work when an incident occurs. Relying on data decryption in the event of a ransomware attack is time-consuming and may not result in usable data. Improper backup recovery procedures contributed to a recent District cyber incident in which it was not possible to recover data promptly to be audited for the ACFR.

Detection and Analysis – It is impossible to develop step-by-step instructions for handling every cyber incident. The Cyber Incident Response Plan should include a process to identify the cyber threat's cause; document the attack's scope, how it occurred, and impacted systems; prioritize the response; and make necessary notifications, including to law enforcement. District agencies experiencing a cyber incident should report it to the Office of Inspector General to coordinate with the appropriate authorities and for awareness purposes to mitigate any impacts to the ACFR.

Containment, Eradication, and Recovery – An organization must develop a containment strategy to prevent further damage once a threat has been identified. Depending on the nature of the incident, this could mean taking actions to remove the hacker from the systems, isolate the compromised systems, or remove the system from the internet. After containing the threat, the incident response team must identify the root cause of the attack, remove any malware or ransomware, and patch any vulnerabilities that were exploited to access the system. Only after the threat has been eradicated can the team bring impacted systems back online. As previously

[8] D.C. OFFICE OF THE CHIEF TECHNOLOGY OFFICER, RISK ASSESSMENT POLICY, (revised May 25, 2021), https://octo.dc.gov/node/1523606 (last visited Feb. 9, 2023).
[9] D.C. OFFICE OF THE CHIEF TECHNOLOGY OFFICER, VULNERABILITY MANAGEMENT POLICY, (revised May 25, 2021), https://octo.dc.gov/node/1523591 (last visited Feb. 9, 2023).

noted, having a working Data Disaster Recovery Plan is critical in recovering from a cyber incident.

Post-Incident Activity – The last step is to review the incident and the effectiveness of the Cyber Incident Response Plan to determine lessons learned and opportunities for improvement. This phase aims to identify any actions needed to prevent future cyber incidents or improve the agency's cyber posture and response to future cyber incidents. Finally, agencies must implement an evidence retention policy that mandates the period agencies must retain evidence from a cyber incident. Evidence retention should consider input from law enforcement and any legal requirements that may govern compromised data, including requirements to notify impacted individuals.

Conclusion

District agencies must remain vigilant against cyber threats by constantly monitoring their systems, patching detected vulnerabilities, and regularly maintaining and testing data system backups. By developing an effective Cyber Incident Response Plan, including a Data Disaster Recovery Plan and Evidence Retention Policy, District agencies can mitigate the risks of cyber incidents that may impact District operations. Finally, as previously stated, District agencies should immediately report all cyber incidents to the Office of the Inspector General at 202-727-1015 when they occur.

If you have any questions, please call James Duginske, Assistant Inspector General for Risk Assessment and Future Planning at 202-727-1015 or email james.duginske@dc.gov.

Thank you in advance for your attention to these matters and your continued support of good governance in the District of Columbia government.

Sincerely,

DWLucas

Daniel W. Lucas
Inspector General

DWL/jpd

cc: District of Columbia Agency Heads