2 Broadway
New York, NY 10004
212 878-7000 Tel

Metropolitan Transportation Authority
State of New York

Cybersecurity Notice

Dear MTA Vendors, Contractors, Consultants and other Partners:

The Metropolitan Transportation Authority, its subsidiaries and affiliated agencies (collectively, the "MTA"), has been working to keep pace with today's dynamic and increasingly sophisticated cyber threat environment. Threats and actual cyber-attacks have been escalating throughout the world since the pandemic began. In 2021, malicious cyber-attacks are more frequent, intense, and potentially impactful. Our highly connected world and the new vulnerabilities in today's telecommuting / remote work environment create more opportunities for cyber criminals. President Biden's May 12, 2021 Executive Order No. 14028, Improving the Nation's Cybersecurity, provides that the Federal Government's scope of protection and security include systems that (a) process data (information technology (IT)) and (b) run the vital machinery that ensures safe operation (operational technology (OT)) including IT and OT in transit systems and operations. The prevention, detection, assessment, and remediation of cyber incidents are top priorities.

Accordingly, in conjunction with the MTA's cybersecurity awareness efforts, we are writing to remind you of the urgent need for you to be vigilant with regard to cybersecurity. Contractors (and their respective subcontractors, subconsultants and suppliers, and all other downstream parties, regardless of tier) that access or maintain the MTA's sensitive or confidential files, information or other data in any form or format (collectively, "Protected Data"), or access, connect to, integrate with or maintain MTA systems, must take all necessary steps to ensure the security of such Protected Data and systems in accordance with all applicable legal requirements, guidelines and contractual requirements. To the extent not otherwise required, we urge you to comply with industry standards and best practices, such as the National Institute of Standards and Technology Cybersecurity Framework.

Together, we can stop the bad actors and protect critical infrastructure. Given your relationship with the MTA as a strategic business partner, and in accordance with your contract requirements, legal requirements and/or best practices, please be reminded that you are required to:

- Use authorized means of connecting to the MTA networks and systems, such as access control, authentication/password policy and management, user access/activity logging and auditing, and communication restrictions
- Have in place or implement a written information security program to keep up with cyber threats and regularly update your written information security program
- Exercise, at a minimum, industry standard cybersecurity measures
- Exercise proactive detection of cybersecurity vulnerabilities and incidents on your networks
- Ensure implementation of appropriate administrative, technical, and physical controls to safeguard the Protected Data

- Ensure that users in your organization are aware of cybersecurity requirements, best practices and policy compliance

- Enforce strong passwords and two factor authentication for authorized access to the MTA networks and systems, and networks and systems within your organization

- Report any known or suspected cybersecurity breach, destruction, loss, unauthorized distribution, use, unauthorized access, disablement, misappropriation or unauthorized modification, or other compromise or misuse of the Protected Data or MTA systems (any of the preceding – an "Information Security Incident") to MTA IT Security at ThreatIntel@mtahq.org immediately and no later than one (1) day after discovery. In reporting a known or suspected cybersecurity breach, such report must identify (a) the nature of the unauthorized access, use or disclosure; (b) the Protected Data accessed, used or disclosed; (c) the identity of all person(s) who accessed, used, disclosed and/or received Protected Data (if known); (d) the actions the Contractor has taken or will take to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (e) the corrective action the Contractor has taken or will take to prevent future unauthorized access, use or disclosure. Contractors shall provide regular updates to the MTA regarding the investigation of and response to any actual or suspected Information Security Incident until the incident is resolved. In addition to notifying the MTA, Contractors shall coordinate with the MTA in their responses to any actual or suspected Information Security Incident. Contractors are expected to fully cooperate – and ensure that all downstream third parties cooperate – with the requests of the MTA, including help with identifying the nature, impact, cause, and severity of any Information Security Incident.

As cybersecurity is increasingly affecting all areas of the business community, you should expect further communication from us on this issue. We urge you to also independently stay informed on the latest cybersecurity threats by reading the ***CISA Alerts*** posted on the Cybersecurity and Infrastructure Security Agency website (us-cert.cisa.gov/ncas/alerts), with particular focus on Alert AA21-148A (Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs and NGOs).

If you have any questions, please do not hesitate to reach out to the MTA via email at MTA-ITSEC-TPRM@mtahq.org. Thank you for your continued attention to this important matter.