MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

January 9, 2017

Mr. Paul J. Wiedefeld
General Manager
Washington Metropolitan Area Transit Authority
600 5th Street NW
Washington, D.C. 20001

Dear Mr. Wiedefeld,

I would like to congratulate you on your recent one-year anniversary as General Manager of the Washington Metropolitan Area Transit Authority (WMATA). You have brought needed leadership to an important regional transit system upon which hundreds of thousands of commuters depend. As you continue to work to prioritize safety, I write to raise three areas of concern – issues of cybersecurity, WMATA's efforts to build-out wireless communication systems and launch a public Wi-Fi network, and the status of efforts to responsibly address first-responder interoperability concerns raised in the wake of the fatal smoke incident at L'Enfant Plaza on Jan. 12, 2015.

On November 25th the San Francisco Municipal Transportation Agency (SFMTA) experienced a debilitating cyberattack that left its computer systems inoperable, forcing the agency to forgo thousands of dollars in collected fares. The incident also may have resulted in the breach of personal information of thousands of employees and customers. Reports have revealed that the attackers, who reportedly were based outside of the United States, were demanding 100 Bitcoins, or around $73,000, in ransom payment.

The frequency of ransomware attacks has grown dramatically in recent years, increasing from around 1,000 attacks per day in 2015 to over 4,000 attacks per day in the first quarter of 2016. Ransomware attacks often target legacy systems that users have failed to update or that are so old they no longer receive patches from the original vendor. If these efforts are directed toward critical infrastructure, the impacts could be grave and far reaching. Should a cyberattack cripple WMATA's ability to collect fares for days at a time, or have the effect of deterring alarmed riders, the financial implications would only exacerbate WMATA's serious and mounting fiscal problems. A cyberattack could potentially threaten these vital networks as well, putting riders at risk if an accident or emergency were to occur during a cyberattack.

As a co-founder of the Senate Cybersecurity Caucus and a staunch supporter of WMATA, I am acutely concerned about what this kind of attack may mean for transportation systems like WMATA. While early reports indicate that the attack on SFMTA may have been opportunistic rather than targeted, I am concerned-that WMATA may represent a particularly enticing target for more advanced threats, given its importance to the region and the number of federal agencies that rely on the system to transport their workforces each day. Given these concerns, I have

included a number of questions below to which I hope you will provide answers by February 15, 2017.

1. SFMTA was apparently a victim of a random attack that looked for antiquated, vulnerable computer systems. When was the last complete overhaul of WMATA's IT systems? Has WMATA identified any end-of-life legacy components, and if so has WMATA taken steps to replace and/or isolate them? Does WMATA have backup systems in place that would allow for some level of continuity of operations in the case of a complete computer system outage?

2. Does WMATA employ network segmentation, including between consumer-facing or internet-connected systems and mission-critical, operational systems to protect against lateral movement of attackers? Does WMATA have a procedure in place to notify overseers, regulators, and the public in the case of a cyberattack?

3. Does WMATA have a comprehensive plan in place to deal with ransomware attacks? If so, was the plan developed in coordination with local and regional partners, including any entities or jurisdictions that may share or have access to internet-connected systems?

Secondly, I understand WMATA and the carrier consortium are implementing an agreement to jointly install the new underground cellular system, which is a positive step forward. I wish to request an updated plan and timeline for the build-out of the wireless communication network within WMATA's underground rail network. The recent announcement of a small (1.1 mile) portion of new infrastructure to enable commercial wireless service between the Potomac Avenue and Stadium-Armory stations represents long-awaited progress. However, work on this network has taken place over several years with very little wireless coverage to show for it today, and WMATA has missed several internal and Congressionally-mandated deadlines. Constituents are rightly concerned about the pace of implementation and the safety concerns that the lack of cell phone service raises. Given the numerous delays over the past several years, I request an updated and realistic schedule for completion of the underground wireless network, and how that work could be impacted or accelerated given the planned service cuts that will reduce hours of operation within the system's tunnels.

WMATA's recently announced plan to install public access Wi-Fi at all underground stations could help address some of the consternation riders have with lack of cell phone service. Providing Wi-Fi coverage within stations, however, should not distract WMATA from the original objective of enabling wireless coverage throughout WMATA's network. Further, without proper management, public Wi-Fi networks can present attractive targets for hackers exploiting flaws in Wi-Fi routers. WMATA should evaluate air gaps, or other measures, to ensure that its public Wi-Fi network is isolated from its secure and mission-critical networks.

Finally, I request an update on work completed as a result of my January 22, 2015 letter on interoperability of public safety communications systems and emergency response training and coordination. As you may recall, my letter was prompted by the fatal Jan. 12, 2015 incident, during which interoperability problems prevented fire and rescue personnel from communicating with Metro officials at the scene of the emergency. I appreciate the report and testing results that

you prepared in response, with the assistance of the Council of Governments (COG) and partner jurisdictions, as well as the agreement to conduct regular and frequent joint training exercises. I ask that, together with COG, you provide an updated report on testing of emergency radio equipment and repeater systems to ensure that there is adequate coverage for effective radio communication in the unfortunate case of another safety incident. Frequent testing to ensure interoperability and seamless communication is particularly important in portions of the system undergoing upgrades to WMATA's new 700 MHz radio system where there may be overlap with the older system currently in place. In addition, I ask that you provide an updated and realistic schedule for both near-term upgrades to the system as well as for integration of the long-term, next generation system, including how that work may be impacted or accelerated through the planned service cuts.

Thank you for your attention to these critical matters. I remain committed to working with the region's Congressional delegation to uphold the federal government's commitment as part of the ten-year, $1.5 billion capital improvement program. Looking forward, it is my hope we can continue to work together to improve WMATA for all of its riders through increased safety, more reliable service and strengthened cybersecurity.

Sincerely,

MARK R. WARNER
U.S. Senator

cc: Roger Berliner, Chairman, Metropolitan Washington Council of Governments
Chuck Bean, Executive Director, Metropolitan Washington Council of Governments
Stuart Freudberg, Deputy Executive Director, Metropolitan Washington Council of Governments