**M E M O R A N D U M** **October 21, 2020**

**TO:** The Honorable Chair and Members of The School Board of Miami-Dade County, Florida

**FROM:** Alberto M. Carvalho, Superintendent of Schools

**SUBJECT:** **STAFF FOLLOW-UP: SCHOOL BOARD MEETING OF SEPTEMBER 9, 2020, AGENDA ITEM H-17, IMPACT OF RECENT CYBER SECURITY ATTACKS ON MIAMI-DADE COUNTY PUBLIC SCHOOLS (M-DCPS)**

At the School Board meeting of September 9, 2020, the Board approved Agenda Item H-17, proffered by School Board Member Ms. Mari Tere Rojas and co-sponsored by School Board Chair Ms. Perla Tabares Hantman, School Board Vice Chair Dr. Steve Gallon III, and School Board Member Dr. Dorothy Bendross-Mindingall. This item requested the Superintendent to provide the Board with an updated review of current network security practices; a complete and accountable response about the recent cyber-attacks, including responsible vendors and actions taken or to be taken; review of current and future staffing needs in Information Technology Services (ITS), review and needs of appropriate equipment currently housed at ITS supporting network security systems; Miami-Dade County Public Schools (M-DCPS) financial investment in ITS for the past five years; updated ITS recovery plan; and provide a report to the Board by October 21, 2020. The purpose of this memo is to provide a detailed report to address the information requested in this item.

**Updated Review of Current Network Security Practices**

The District's holistic approach to cybersecurity consists of proactive systems and processes that protect our networked resources while maintaining the flexibility to respond to issues when necessary. This requires the use of strategies that are continually refined to match the ever-changing world of cyber threats. There is a delicate balance between facilitating convenient access to resources while attempting to protect those resources. Therefore, options to allow for these seemingly disparate goals are constantly being researched, evaluated, and implemented where appropriate and financially feasible. ITS is currently performing a comprehensive review of systems, applications, infrastructure, and processes to identify potential security concerns and gaps. We will continue to implement zero/low-cost solutions as appropriate, but many of these solutions have a limited impact on an organization's overall security. Ultimately, cybersecurity initiatives generally require a combination of culture change coupled with a significant financial investment. Regardless of what technical approaches to cybersecurity are utilized, the District must have a renewed focus on user awareness in order to complement any additional controls implemented.

In an effort to validate our current approach to security and to identify any potential gaps, the District has entered into agreements with third-party entities to perform a thorough evaluation of our network environment and current cybersecurity measures, including policies and procedures along with current hardware and software solutions. Included among the experts assisting with the district technology review are representatives from Appgate (a cybersecurity firm backed by information technology magnate Manny Medina), Microsoft, Cisco, HP, IBM, Comcast, VMWare, DigitalEra, UDT, BlackBerry, Trend Micro,

Sand Vine, AT&T, F5, and Fortinet. These entities comprise a panel of industry leaders in technology, particularly in the cybersecurity space, and we are confident that this collaboration will ensure that the District's current and future security practices will continue to meet or exceed industry best practices. Recommendations stemming from these engagements will be shared with the Board as appropriate and will result in a cybersecurity strategy that will balance resources with risks that will require additional budgetary commitments to address any potential gaps.

**Recent Cyber-Attacks**

Beginning the morning of August 31, 2020, M-DCPS was targeted by multiple DDoS (Distributed Denial of Service) attacks which continued over the course of the first week of school. Attacks of this nature are intended to disrupt the communications between the District and the Internet. The District's Internet Service Provider (ISP), Comcast, is contracted to provide automatic mitigation services for M-DCPS. Since the attacks, Comcast has improved notification procedures and provided extended mitigation services to prevent disruptions caused by DDoS attacks directed at the District. In addition, the District is working with cybersecurity consulting firms and District technology partners to identify gaps as well as ensure resource availability and network health. During these ongoing engagements, they have found no evidence of a breach or compromise of data as a result of the attacks.

**Review of Current and Future Staffing Needs in Information Technology Services**

ITS has 485 staff members, 200 of which are support technicians and 26 are Data Center staff. There are currently 4 open positions in the area of data security.

As conveyed to the Board on September 10, 2020, ITS is reviewing and revising its job descriptions to compete with high-tech industry standards.

Competitive private sector compensation makes it difficult to attract and retain effective IT staff. For that reason, ITS often hires, trains, and promotes from within, bringing in staff at lower pay grades and then promoting staff as their skills improve. However, in November 2018, working in collaboration with the Office of Human Capital Management, ITS re-aligned to create the department, Data Security, Governance and Compliance, and added 12 new technical positions including SAP, Web & Mobile Development with more competitive salaries. While we realize that it may not be plausible to compete with private sector salaries, it is our goal to compete with other public sector jobs within the Florida Retirement System (FRS).

In addition, ITS works collaboratively with the Miami-Dade Schools Police Department (MDSPD) to augment the District's cybersecurity efforts. MDSPD has proven to be an asset in the fight against cybercrime by providing assistance with combating and investigating elements of cyber-attacks. MDSPD maintains a Certified Forensic Computer Examiner on staff (International Association for Computer Investigative Specialists), and, through partnerships with the FBI Cyber US Secret Service Task Forces provides actionable intelligence used by the District to stay up to date with emerging threats where applicable.

MDSPD has also been integral in the promotion of the "See Something, Say Something" Campaign along with social media awareness efforts during presentations to school-site

faculty and staff as well as students. Awareness efforts continue outside of the school environment where the Department encourages parents to discuss the dangers of social media with their children and to monitor the use of their child's smart device. Additional functions performed by MDSPD to keep our students safe include following up on online Fortify tips and cyber tips from the National Center for Missing and Exploited Children, along with supporting the efforts of the Internet Crimes against Children Task Force (ICAC), which investigates child exploitation.

**Review and Needs of Appropriate Equipment Currently Housed at ITS Supporting Network Security Systems**

The Data Security, Governance & Compliance and Network, Cybersecurity, and Technical Services (NCATS) departments are responsible for overseeing and managing the District's network security and policies. Data Security, Governance & Compliance is responsible for establishing and managing the policies and procedures for securing the District's networked resources. Proper governance ensures that the legal and ethical obligations of the District are met and that business functions can be standardized and streamlined to ensure efficiency. NCATS is responsible for the confidentiality, integrity, and availability of the District's enterprise information systems in both the physical data center and in the public cloud.

The ITS data center supports outgoing connections to over 400 District sites and provides centralization for Internet as well as on-premise enterprise applications comprised of more than 1,200 virtual servers. Additionally, ITS manages over 200,000 devices that connect to our systems and accommodates an estimated 300,000 personal devices that are supported at M-DCPS locations. Specifics regarding network infrastructure and related solutions cannot be made available in order to ensure system integrity and security.

Based on the security assessment from Appgate and the compromise assessment from Blackberry, we will develop and implement a cybersecurity plan that will use funds identified for cybersecurity technology. Identified needs will be reported to the Board at the conclusion of those reviews.

**M-DCPS Financial Investment in ITS for the Past Five Years**

The average yearly budget received for the last five years for hardware/software maintenance has been $13,500,009.

In addition to the yearly maintenance funds, ITS has received funds to support a variety of IT enhancements as summarized below. This does not include grant funds that went to ITS, salaries, capital funds used to purchase computers and other IT items during construction, and cost of purchasing computers and devices for Digital Convergence and the move to distance learning.

- **FY1617**
  - $900,000 – Batteries, battery monitoring system for Uninterrupted Power Supply, risk assessment, switches

- **FY1718**
  - $300,000 – UPS Replacement in ITS Data Center

- $360,000 – Mainframe Terminal Session Replacement – Rocket Bluezone
- $100,000 – SharePoint 2007-2010 Migration

- **FY1819**
  - $150,000 – Anti-Virus protection for District computers
  - $500,000 – 995 Phone System Replacement
  - $55,000 – Travel System upgrade to SAP

- **FY1920**
  - $499,219 – IBM Tape Drives upgrade – funded by Capital

- **FY2021**
  - Budget under consideration

**E-Rate Funding FY1617-FY2021**

- District Spend – $1,221,965.07
- E-rate Approved Amount – $5,662,636.17
  - Wireless
  - Wiring

**Updated ITS Recovery Plan**

Pursuant to a finding from the Florida State Auditor General, an updated Disaster Recovery Plan is currently in progress and should be substantially complete by December 2020.

If you have any questions or require additional information, please contact Mr. Eugene P. Baker, Chief Information Officer, Information Technology Services, at 305 995-3754.

AMC:mdr
M389

cc: School Board Attorney
Superintendent's Cabinet
Mr. Eugene P. Baker
School Board Agenda Office