City of Lowell
Management Information Systems
375 Merrimack Street • Lowell, MA 01852
P: 978.674-4099 • F: 978.970.4004 • www.lowellma.gov

Mirán Fernandez
Chief Information Officer
Cable TV Coordinator

John Meyers
MIS Director

MEMORANDUM

TO: Eileen Donoghue, City Manager EMD

FROM: Mirán Fernandez, Chief Information Officer

DATE: October 12, 2021

Re: **MOTION RESPONSE: 07/27/2021 by C. Conway** – Req. City Mgr. Report On City's Plan Against A "Ransomware Attack" That Will Ensure That All City Departments Have Sufficient Protocols And Updated Technology To Prevent Hackers From Compromising Our Systems; To Further Ensure That There Is Sufficient Security On The City's Voting And Tabulating Machines."

Advances in technology have offered municipalities the opportunity to make everyone's life less stressful by providing quick and easy ways to accept online payments, along with efficient ways to issue permits and other services. As the threat of cyber-attacks on municipalities designed to disrupt these opportunities continue to increase, many municipalities have adopted a minimum cybersecurity baseline.

The City of Lowell's MIS Department has adopted a baseline designed to improve our overall cybersecurity posture by (1) training employees, (2) sharing in local/ state/ regional threat information, (3) creating a plan to assist with minimizing disruption of our technology and data, and (4) implementing best practices designed to secure our technology and data.

With respect to the city's voting and tabulating machines, none of the equipment currently in use is connected to any shared network through which any hackers might be able to disrupt the election process. From the time the tabulation machines are deployed to polling location until the time that they are returned to the Elections Department, machines are under physical observation. Output from the tabulation machines is physically cross checked multiple times prior to being entered into the Commonwealth's private/ secured election system.

If it is the wish of the Council, MIS welcomes the opportunity to discuss the strategies and approaches taken via Executive Session, in order to avoid shining a spotlight on our operations which might attract hackers wanting to target specific systems, initiatives, or programs.