Memorandum

CITY OF DALLAS

DATE April 3, 2015

TO Members of the Budget, Finance & Audit Committee: Jerry R. Allen (Chair), Jennifer Staubach Gates (Vice-Chair), Tennell Atkins, Sheffie Kadane, Philip T. Kingston

SUBJECT Upcoming Agenda Item: Acquisition of the New Cybersecurity Threat Protection System

The April 8, 2015 Council Agenda will include an item to award a contract to purchase the FireEye Dynamic Threat Intelligence system (hardware and software) including maintenance and support for a three-year period to Solid Border in an amount not to exceed $100,390.00.

The FireEye Dynamic Threat Intelligence system is a real-time cybersecurity detection system which analyzes the behavior of computer data as it enters the City's network. If the behavior of the data is not recognized, the system does not allow the data onto the City's network. The data never reaches a computer. This is different from other threat detection technologies which are file signature-based such as McAfee antivirus and malware products. These file signature-based technologies analyze data after it enters the City's network as it is loaded onto a computer. If an unknown file signature is detected, the file is removed from the computing device.

Procuring the FireEye system provides an additional layer of security protection needed to prevent repeated attempts by hackers to gain a foothold inside the City's network. Once inside the City's network, hackers can illegally obtain information, disrupt critical computer system operations including SCADA-based computer systems (such as those systems operated by Dallas Water Utilities and Trinity Watershed Management), and position malware within the City's network to carry out a cybersecurity attack in the future.

Examples of illegal, destructive, and disruptive activities caused by cybersecurity attacks include, but are not limited to:

- Retrieving confidential information from computers such as HIPAA-protected patient health records at DFR, CJIS-protected law enforcement data at DPD, Personally Identifiable Information (PII) such as social security number, home address, and telephone number, computer user account IDs, and system passwords
- Intentionally destroying data on computers
- Intentionally causing networks and computers to malfunction and fail
- Undermining aspects of mission-critical services including first responder services provided through Computer-aided Dispatch, the City's radio network, etc.

The FireEye Dynamic Threat Intelligence system will enhance the ability to control and protect the City from harmful and illegal activities performed by computer hackers.

Please contact Bill Finch at 670-1890 if you have any questions.

Jill A. Jordan, P.E.,
Assistant City Manager

c: Honorable Mayor and Members of the City Council
    A.C. Gonzalez, City Manager
    Warren M.S. Ernst, City Attorney
    Craig D. Kinton, City Auditor
    Rosa A. Rios, City Secretary
    Daniel F. Solis, Administrative Judge
    Ryan S. Evans, First Assistant City Manager

    Eric D. Campbell, Assistant City Manager
    Mark McDaniel, Assistant City Manager
    Joey Zapata, Assistant City Manager
    Jeanne Chipperfield, Chief Financial Officer
    Sana Syed, Public Information Officer
    Elsa Cantu, Assistant to the City Manager – Mayor & Council
    William Finch, CIO/Director Communications & Information Systems