I. EXECUTIVE SUMMARY

In accordance with our audit plan for the fiscal year ended June 30, 2015, we completed a high level review in June 2015 of the Metro Hartford Innovation Services (MHIS) Network Security. The purpose of the review was to evaluate MHIS network security and make appropriate recommendations. We reviewed the results of our examination with S. Sitaru, Chief Innovation Officer (CIO); and, other responsible members of management. MHIS management has also noted actions taken or planned including timeframes to resolve each finding and/or recommendation in this report. We thank MHIS management for their cooperation and courtesies extended to us during our audit.

Background

MHIS supports both the City of Hartford (the City) and the Hartford Public Schools (HPS) and is aligned with core strategic objectives of the Mayor. Core systems include the City’s Financial systems MUNIS and Quality (Tax and Assessor system), and the HPS’s PowerSchool system. The MUNIS system was previously maintained on City servers, but was migrated to the Tyler Cloud on April 4, 2015. The strategic mission of MHIS is to provide leadership, coordination, and support for the information technology and communication needs of the City, HPS and the Hartford Public Library. The MHIS infrastructure consists of a data center, about 300 servers and about 17,000 desktops/laptops, which primarily run on Windows based operating systems. There are about 100 sites covered by the network and MHIS uses a five year life cycle on all hardware. The HPS is now using Microsoft Office 365 and the City will convert over to this platform later in 2015. Microsoft Office 365 had significant improvements in data security over previous versions of Microsoft Office.

General

In general, MHIS has numerous areas that need attention relating to Organizational Management, Personnel Practices, System Access Controls, Physical Security, and Data Security as noted in the details of this report.

Scope

We performed a high level network security review of the existing policies, procedures and controls through the use of comprehensive internal control and risk assessment questionnaires and physical observations of facilities. We did not perform any system penetration tests nor did we test employee system access controls. The latter is performed as part of our regularly scheduled audits during the year.
II. AUDIT RESULTS

Organizational and Management Practices

Management has recently hired a Network Security Engineer who will work with the CIO to follow-up and resolve all of the issues noted in this report. Management has somewhat assigned roles and responsibilities for information security across MHIS and is currently addressing the Mayor’s Executive Order on Cyber Security. However, we noted the following:

- Information security risk assessment is an on-going process of discovering, correcting and preventing security problems. Information security risk assessments are an integral part of a risk management process designed to provide for and maintain appropriate levels of security for information systems. Periodic information security risk assessments are part of sound security practices and are industry best practices. MHIS has not implemented such a process. The risk assessment will help determine the acceptable level of risk and the resulting security requirements for each system and then implement and monitor a set of security measures to address the level of identified risk. For a new system, the risk assessment is typically conducted at the beginning of the System Development Life Cycle (SDLC). For an existing system, risk assessments may be conducted on a regular basis throughout the SDLC and/or on an ad-hoc basis in response to specific events such as when major modifications are made to the system's environment or in response to a security incident or audit. Quality, implemented in late 2014, is a perfect example where a security risk assessment was not performed by MHIS.

- There is no formal document that provides management with an overview of the security requirements for all systems including a description of existing security controls to this system. Also, management should, but does not formally assess the effectiveness of the controls at least annually, especially for new systems such as Quality.

- Network and communication protection policies and procedures relating to authorization to network connections to sensitive and critical business applications are not in place.

- Policies and procedures relating to technology upgrades, network equipment, firewall and server configurations are not in place.

- MHIS currently does not support the Quality system nor do they control data access, system changes or any other critical data security controls. All support is supplied by the system vendor through the City Tax Collector. This is a significant weakness in the network security controls.

- Changes made to information systems are not adequately controlled, tracked and documented nor are they formally reviewed and approved where required. There is no formal policy for system change controls.
City of Hartford
Metro Hartford Innovation Services
Network Security Audit

- There are no vulnerability scanning tools or techniques used to periodically evaluate system configurations and services for known vulnerabilities.
- Policies and procedures covering data classification, such as its value, legal requirements, sensitivity and importance to the City are not in place.
- The City currently has no Cyber Liability Insurance.

We recommend that MHIS management take action to follow-up on and address the areas of concern detailed above.

Management Response:

Due Date: August 31, 2015
Responsible Person: Sabina Sitariu, Chief Innovation Officer

- The Network Security Engineer has already identified various security issues and is in the process of completing a Risk Assessment.
- The Network Security Engineer is in the process of creating a formal document that provides management with an overview of the security requirements for all systems including a description of existing security controls.
- The Network and Applications Security Awareness Team (NASA), a group of MHIS staff and others from outside the department will develop and document policies and procedures relating to authorization to connect to sensitive and critical business applications.
- The NASA Team will develop and document policies and procedures relating to technology upgrades, network equipment, firewall and server.
- MHIS currently supports the infrastructure side of the Quality Tax System. The server is hosted by MHIS and database maintenance is done periodically. MHIS does not support the front end of the application and in order to do so would need additional staffing.
- The NASA Team will develop a policy for system change controls and create a mechanism to where changes are controlled, tracked and documented appropriately.
- The Network Security Engineer is tasked with making recommendations and implementing various vulnerability scanning tools. He has already identified tools we can activate on our network firewall system. The Director of Support Services is in the process of implementing Microsoft System Center Configuration Manager which came with the School Districts Enterprise Microsoft subscription and will be included in the Office 365 purchase for the City. This is a desktop and user management system which has many built in security tools to manage and monitor
the various computers and devices used in the school district and city. It also monitors and records user activity and identifies irregularities. The implementation of Office 365 for the City is scheduled this fall.

- The NASA Team will create a plan to create policies and procedures covering data classification, such as its value, legal requirements, sensitivity and importance to the City. This is a large undertaking and may require additional resources that will be identified in the plan.

- Cyber Liability Insurance has been explored with the School District, but MHIS was advised to first complete all the above. The cost of the insurance for the School District was identified to cost in the range of $80,000. That money would be better spent on implementing all of the above and once complete could result in a lower premium.

Personnel Practices

A process to terminate an employee’s information system physical access when an employee changes assignments or terminates employment is in place. Background checks are required on employees who work with or have access to confidential, sensitive information or critical systems. Best practices would require periodically performing background checks on those employees. However, we noted the following:

- Security awareness training for all CITY and HPS employees is a best practice that is not in place. The training should address acceptable use and good computing practices for systems they are authorized to access in accordance with existing documented policies such as privacy requirements to personal identifiable information, virus protection, incident reporting, internet use, monitoring activities, password requirements and consequences of legal and policy violations.

- Policies and procedures that address an employee’s roles and responsibilities and compliance to security requirements such as access rights and disciplinary processes are not documented and in place.

- Procedures for identifying system access needs by job function and screening criteria for employees performing those functions are not documented and in place for crucial systems, except for MUNIS.

We recommend that MHIS management take action to follow-up on and address the areas of concern detailed above.

Management Response:

Due Date: August 31, 2015
Responsible Person: Sabina Sitaru, Chief Innovation Officer
MHIS ran a cyber-security awareness program during the month of October 2014 and will run the program again in October 2015 which is designated as National Cyber Security Awareness Month. MHIS is also exploring training programs which can be run continuously. Cost is a factor and funds will need to be identified.

The NASA Team will work with departments/management on developing policies and procedures that address an employee’s roles and responsibilities along with compliance to security requirements such as access rights and disciplinary processes.

The NASA Team will work with various system managers on procedures for identifying system access needs by job function and screening criteria for employees performing those functions. Example - PowerSchool, Quality, etc.

System Access Controls

System access controls are routinely tested by us during our audits performed in accordance with our yearly audit plan. During this review, we did not test these controls but we did notice that password controls could be enhanced by requiring strong passwords be used and establish a policy that password are not to be shared.

We recommend that MHIS management take action to follow-up on and address the areas of concern detailed above.

Management Response:

Due Date: August 31, 2015
Responsible Person: Sabina Sitaru, Chief Innovation Officer

MHIS is working on implementing stronger passwords and promoting user awareness on not sharing passwords. We have implemented a stronger password system with the migration of MUNIS to the cloud. The Cyber Security Executive order outlines the do’s and do not’s including the sharing of passwords or storing them in an unsecured location like under a keyboard.

Physical Security

The data centers are access protected, have fire detection and suppression, temperature and humidity controls and water damage detection. Physical access to data center facilities is controlled and individual access authorization is verified before granting access. A process is in place to permanently remove any sensitive data and licensed software prior to disposal of any electronic equipment. However, we noted the following:
• There are no documented policies or procedures that address the purpose, scope, roles, responsibilities and compliance for the physical and environmental security, entry controls, room temperature controls, fire suppression and equipment and cabling controls in the data center.

• There is no auxiliary power back up for the data center located at MHIS in Constitution Plaza.

We recommend that MHIS management take action to follow-up on and address the areas of concern detailed above.

Management Response:

Due Date: August 31, 2015
Responsible Person: Sabina Sitaru, Chief Innovation Officer

• The Data Center Manager will develop and document a policy or a procedure that addresses the purpose, scope, roles, responsibilities and compliance for the physical and environmental security, entry controls, room temperature controls, fire suppression and equipment and cabling controls in the data center.

• There is a Universal Power Supply (UPS) in the data center; however it will only supply power for a few hours. It is 13 years old and is in need of replacement. This was recently identified and the Data Center Manager has been tasked with developing a recommendation for replacement of the UPS and on moving equipment to the Public Safety facilities and or cloud storage such as Microsoft Azure where there is auxiliary power. The cost of installing Auxiliary power to the leased space at 260 Constitution Plaza would cost in the range of $100,000. It has been identified by the Data Center Manager that in an emergency we can contact a vendor to deliver and setup a generator. He is exploring the mechanics of the setup. We would need to have the vendor on contract with specific guidelines for delivery in the event of an emergency.

Data Security

City and HPS systems activity and processing is routinely backed up daily to offsite servers and on backup tapes located in various secured City locations. Backup copies of information and software are completed on a routine schedule, tested regularly and stored off-site. However, we noted the following:

• A formal disaster recovery plan including procedures to update the plan and periodically test it has not been established. A disaster recovery plan supports the current business continuity of the City.

• Policies and procedures relating to the protection of data on electronic storage media such as CD’s, USB devices etc. are not in place.
City of Hartford  
Metro Hartford Innovation Services  
Network Security Audit

- Mobile and portable systems and their respective data are not protected by way of encryption, physical security and secured passwords.

- Sensitive data is not protected from unauthorized disclosure during transmission, such as email transmitted data. Office 365, which is implemented in HPS and soon to be implemented in the City, protects this data from unauthorized disclosure.

- Sensitive data should be stored on separate pre-defined servers for additional security and for backup and recovery purposes.

We recommend that MHIS management take action to follow-up on and address the areas of concern detailed above.

Management Response:

Due Date: August 31, 2015  
Responsible Person: Sabina Sitaru, Chief Innovation Officer

- The NASA Team will create a formal disaster recovery plan including procedures to update the plan, along with periodically testing.

- The NASA Team will develop and document policies and procedures relating to the protection of data on electronic storage media such as CD’s, USB devices etc.

- The NASA Team will create a plan and identify systems along with any costs that we can implement to secure mobile and portable systems and data by way of encryption, physical security, and secured passwords.

- The NASA Team will create a plan to identify sensitive data and determine storage, security, backup, and recovery needs along with any costs associated with identification, storage, backup, and recovery.
City of Hartford
Metro Hartford Innovation Services
Network Security Audit

Distribution:

City Council Members
Internal Audit Commission Members
P. Campbell, Chief Auditor
A. Cloud, City Treasurer
J. Figueroa, Chief of Staff, Mayor’s Office
D. Hill, Chief Operating Officer
J. Mazzuoccolo, Manager, McGladrey LLP
L. A. Ralls, Acting Director, Finance Department
J. Sanchez, Director, Department of Management, Budget and Grants
P. Segarra, Mayor