

ITS Strategic Roadmap – FY 16

Information Security Management

Author: *Keith Durbin*

Date last updated: *January 23, 2015*

Background

The Information Security Management program, created by Executive Order 38, strives to provide the policy and guidance to safeguard the confidentiality, availability and integrity of the Metropolitan Government's information assets and infrastructure.

Program activities include policy creation, distribution, review and assistance with compliance; guidance on compliance with targeted Federal and State regulations, including HIPAA; information security awareness and training; and identification and remediation of information security risks.

The Information Security Management program exists to serve to all Metropolitan Government employees and third party users except those agencies specifically outlined in Executive Order 38. Those agencies, however, are requested to consider adopting policies and practices put forth through this program.

Stakeholders are all Departments and Agencies of the Metropolitan Government; government vendors and partners; the members of the Mayoral Information Security Advisory Board; and the citizens of Nashville and Davidson County.

Current Strategic Drivers

1. **Public demand for Secure Government Systems (High)** – the proliferation of public awareness of the vulnerability of systems which maintain their critical health, financial, educational and other records has heightened awareness and fear of loss. Additionally the public increasingly desires to see evidence of effectiveness of the program.
2. **Customer Demand for Efficient, Timely Solutions (High)** – Customer departments and agencies want to implement technology that efficiently meets their business needs. IT Security can be seen as an impediment to timely or efficient solutions.
3. **Environmental Security Threats (High)** - Social Engineering (Phishing, Spear Phishing), Advanced Persistent Threats (APTs), Hacktivist Groups (Anonymous, LulzSec), reconnaissance, and malware will continue to require attention with proper controls through well-constructed and implemented policies, procedures, and standards.
4. **Regulatory Compliance Obligations (High)** – Regulations and standards such as HIPAA/HITECH, PCI-DSS, TCA 47-18-2107, GLBA, and FERPA have specific information security control needs that must be addressed to realize appropriate levels of compliance with applicable laws, standards, and regulations.
5. **Mayoral Executive Orders (High)** – Executive orders 004, 005, 015, and 038 address specific information security areas to include governance, training, acceptable use, and policy development and implementation.



6. **BYOD (Bring Your Own Device) (High)** – Persons bringing their own devices to attach to the Metro network such as iPads, Android based devices, laptops, and smartphones can introduce numerous additional vulnerability vectors that may lead to exploits and information security compromise if not addressed through training and well-constructed and implemented policies, procedures, and standards.
7. **Metro Employee Awareness (High)** – People will continue to be the weak link in the information chain without a constant and evolving information security awareness program.
8. **Cloud Computing (High)** – The widespread public acceptance of cloud for services that employees and citizens use every day, along with the potential for positive financial impact and increasingly effective cloud vendor security stance make a hybrid model a potential direction. Due to these economies of scale and potential cost savings, a growing number of Metro agencies have investigated and/or migrated certain to cloud-based systems.

On the Horizon Strategic Drivers

1. **New Legislation (Medium)** – Proposed legislation, including that proposed by President Obama, would seek to improve the way the government and private sector share information about cyber threats, and would update the legal framework needed to go after cyber criminals. If passed and enacted, these and other laws may have information security implications for Metro Government.
2. **New Controls and Standards (Low)** – Standards that Metro information security policies and procedures are based on, such as NIST and ISO, are constantly being updated.
3. **New Mayoral Administration (Low)** – Depending upon the priorities of the next administration, the direction of the information security management program may be altered to fit his/her agenda.

Short Term Goals (0-6 months) 7/1/15 – 12/31/15

#	Goal/Objective	Est. Start	Est. Duration
1	Initiate and evaluate results of Information Security Management program review and gap analysis.	7/1/2015	6 months
2	Work with Finance Purchasing and Legal Department to complete final review of and fully implement the Information Security Agreement (ISA) and contract components for IT-related procurements.	7/1/2015	3 months
3	Continue to plan and coordinate activities of the outsourced HIPAA Privacy and Security offices for Metro's identified Covered Entities.	7/1/2015	Ongoing
4	Plan and coordinate activities for October 2015 Cyber Security Awareness month.	7/1/2013	4 months
5	Work with new administration to educate on information security risks and review program successes, gaps, goals and objectives.	9/1/2015	1 month



6	Initiate and complete PCI-DSS Security Gap Assessment. Key deliverable to include findings and recommended actions. (Funding Required)	10/1/2015	2 months
---	--	-----------	----------

Medium Term Goals (6-18 months) 1/1/16 – 12/31/16

#	Goal/Objective	Est. Start	Est. Duration
1	Depending on findings, initiate PCI-DSS Security Gap Assessment remediation efforts and develop project plan with key milestone deliverables and dates. (Funding Required)	1/1/2016	6 months
2	Design and test updated risk assessment process. Initiate new risk assessment process within ITS.	3/1/2016	6 months
3	Develop business case for policy/risk management automation. Research industry reports.	3/1/2016	2 months
4	Document Metro-wide information security risk management framework – risk definitions, stakeholders, input sources, lifecycle management, metrics.	3/1/2016	6 months

Long Term Goals (18-36 months) 1/1/17 – 6/30/18

#	Goal/Objective	Est. Start	Est. Duration
1	Refresh HIPAA Security Assessment. (Funding Required)	TBD	TBD
2	Research possibility of implementing GRC (governance, risk management and compliance) solution. (Funding Required)	TBD	TBD

Related Roadmaps:

- Network Security

Other Resources:

- Mayoral Executive Orders 4, 5, 15, 38 at <http://www.nashville.gov/Metro-Clerk/Legal-Resources/Executive-Orders.aspx>
- Metro Government Information Security Policy at <http://www.nashville.gov/Information-Technology-Services/Information-Security/Information-Security-Policies.aspx>

