

# ITS Strategic Roadmap – FY16

## Network Security

Author: *John Griffey*

Date last updated: 1/21/2015

### Background

The security of computer networks and information is a front page topic in the news on a daily basis. Whereas the Information Security Management program established by Executive Order is focused on policy, risk, and awareness, Network Security provides technical services to all Metro departments and agencies to strive to ensure the confidentiality, integrity and availability of Metro's IT resources. This is accomplished through the use of many centralized technical tools that provide technical solutions for policy controls.

These services include, but are not limited to,

- maintaining the security at the network perimeter,
- protecting the Metro network from malware,
- monitoring the Metro network for any security related issues,
- developing security solutions around mobile devices,
- responding to issues that occasionally arise, and
- proactively scanning the Metro network for security issues and correcting those issues.

Key stakeholders are all of Metro departments and agencies who use Metro's wired and wireless network infrastructure, including external entities that may work with those departments and agencies.

### Current Strategic Drivers

1. **Increased customer demand for cloud computing and cloud based services (Game Changing)** – More services are moving to this model.
2. **Customer demand for access to everything, all the time, from any device, from anywhere (Game Changing)** - Addressing security issues around mobile device usage.
3. **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.
4. **Public and customer demand for more secure government systems (High)** – proliferation of mobile devices, rise of hacktivism, reliance on any time connectivity to Metro network, etc. has increased the need to ensure the security of the Metro network. Additionally customers desire to see evidence of effectiveness of the program.
5. **Increased targeting of government (High)** – As Federal, State and Local Governments become more of a target for cybercriminals, it is important to look beyond internal resources and look to partner with third party security services in an effort to keep Metro secure.



6. **Use of hacktivism (social outcry via cybercrime)** (High) – New “hacktivism” movement has set local government as a target. Use of IDS, IPS and better log management needed as additional protections against these external threats
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. **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.

## On the Horizon Strategic Drivers

1. **Proliferation of network connected “things”, aka. “The Internet of Things”** (High) – More everyday objects have network connectivity, allowing them to send and receive data. Security is often an afterthought for these devices so their impact is not known.

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

#	Goal/Objective	Est. Start	Est. Duration
1	Expansion of vulnerability assessment program - develop plan to offer this as a service to other departments and expand assessment scans to desktop systems	7/15	6 months
2	Deploy mobile device management solution – provide method of deploying a set security stance to mobile devices	7/15	12 months
3	Deploy remote access control solution – provide method of discovering mobile devices on the network and deploy a set security stance to them.	7/15	12 months
4	Better define the processes and procedures around use of newly implemented technical controls and third party managed monitoring services to use these to their fullest capacity and realized a full return on investment.	7/15	3 months
5	Identify operational metrics to measure the effectiveness of the current security investments and define for Metro.	10/15	7 months
6	Continue assessing security implications of cloud computing services and work to develop standard security guidelines to be met for the use of such services.	12/15	9 months
7	Review security offerings by currently contracted vendors to help address any vulnerabilities in Metro’s information security program. These would include solutions to bolster Metro’s security awareness program.	12/15	12 months



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

#	Goal/Objective	Est. Start	Est. Duration
1	Assess security implications of network connected devices (“internet of things”) and work to develop standard security guidelines to be met for the use of such devices.	1/16	6 months
2	Development of processes that coordinate with the ITS Telephone, and Networking Services to ensure that security continues to be a component in the planned development of those infrastructures.	1/16	12 months

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

#	Goal/Objective	Est. Start	Est. Duration
1	Feasibility research in the use of data rights management (DRM) solutions for the added protection of Metro data.	1/17	12 months
2	Research conducting an external intrusion detection/vulnerability assessment engagement. Capital funding will be required.	1/17	6 months

#### Related Roadmaps:

- Data Center and Environmentals
- Identity and Access Management
- Information Security Management
- Network Infrastructure
- Wireless Networking

#### Other Resources:

- Metro Government Information Security Policy at <http://infosec.nashville.gov>

