METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 14
SUBJECT: CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING	DISTRIBUTION DATE: 9/28/2017
	EFFECTIVE DATE: 10/15/2017
ISSUING AUTHORITY: DIRECTOR OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to help the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) improve its security posture by the sharing of cyber threat information within the Metropolitan Government, consuming and using cyber threat information received from external sources, and producing cyber threat information that can be shared with other organizations. This policy also defines specific considerations for participation in information sharing communities.

POLICY

1.0 Generally

The Metropolitan Government of Nashville and Davidson County (Metropolitan Government) shall develop processes to facilitate the dissemination of cyber threat intelligence and the sharing of cyber threat information with external entities and partners in an effort to improve the security postures of the cyber community as a whole. By exchanging cyber threat information within a sharing community, Metropolitan Government can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats Metropolitan Government may face. Using this knowledge, Metropolitan Government can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies.

2.0 Detailed

2.1 Metropolitan Government shall identify and document resources to be used to keep informed about information security threats. This cyber threat information should include: indicators of compromise; tactics, techniques, and procedures (TTPs) used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.

2.2 Metropolitan Government shall identify and document resources to be used to keep informed about information security vulnerabilities and obtain timely information about technical vulnerabilities of information systems and applications being used.

2.3 Metropolitan Government shall develop methods for producing and sharing threat information internally. This information should be used to remediate risk and respond to threats.

2.4 Metropolitan Government shall identify appropriate contacts with special interest groups or other specialist security forums and maintain professional associations as a source of security information. External information sharing agreements should be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information. Sensitive Information shall not be shared as part of any information sharing agreements.

2.5 Metropolitan Government shall establish an information sharing plan. The plan should address the collection and analysis of threat information from both internal and external sources and the use of this information in the development and deployment of protective measures. This plan should include considerations with regards to information sharing with external groups, establishing sharing relationships and participating in sharing relationships.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300.

9/27/2017

_____ _____

Keith Durbin
Director of Information Technology Services
Metropolitan Government of Nashville and Davidson County

Date

REFERENCES

- ISO 27002: sections 6.1.4
- NIST Special Publication 800-150, *Guide to Cyber Threat Information Sharing*
- NIST Special Publication 800-53 rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations:* Control numbers – AC-21
- *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- NIST Special Publication (SP) 800-61, *Computer Security Incident Handling Guide*

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	09/09/2017	Original Version