THE RISK MANAGEMENT ASSOCIATION

1801 Market Street, Suite 300 • Philadelphia, PA 19103
215-446-4000 • Fax: 215-446-4101 • www.rmahq.org

ADMINISTRATION ISSUES FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

On February 12, 2014 the National Institute of Standards and Technology issued its "Framework for Improving Critical Infrastructure Cybersecurity". This Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework provides a common mechanism for organizations to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of the following parts:

- **Framework Core**: a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover.
- **Framework Implementation Tiers**: provides context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.
- **Framework Profile**: represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile ("as is" state) with a Target Profile (the "to be" state).

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. A portion of the Framework document presents examples of how it can be used. The Framework is voluntary and includes a set of industry standards and best practices to help organizations manage cybersecurity risks. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The complete Framework report can be found at the following link:
https://www.nist.gov/framework