Discussion Draft
Message to Senior Executives on the Cybersecurity Framework

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. The complexity of our systems, the increased connectivity, and the reliance on technology coupled with an advancing cybersecurity threat now puts our critical infrastructure, our information, and our safety at risk.

The cybersecurity threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. This risk not only affects the nation, but also your business, your employees and the communities that you serve.

Cybersecurity risk is a reality that organizations must understand and manage to the level of fidelity of other business risks that can have critical impacts. Much like reputational, financial, supplier, and other risks, organizations must manage cybersecurity risk in order to gain and maintain customers, reduce cost, increase revenue, and innovate. If your company is publicly traded, for example, your Board of Directors should be aware of cybersecurity risk and the steps your organization must take to manage this risk.

The potential consequences of a cybersecurity incident vary — the impact ranges from the loss of valuable intellectual property to the disruption of critical service delivery. Active threats seek to steal information, destroy data and render critical systems inoperable. Operational errors or natural threats can also negatively impact the operational systems used to deliver critical services.

A Key Tool: the Industry-Led Cybersecurity Framework

Due to these threats, impacts and risk to our nation's economic and national security, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" on February 12, 2013. The Executive Order calls for the development of a voluntary risk-based cybersecurity Framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective", and is developed and implemented in a partnership with owners and operators of the nation's critical infrastructure.

The Framework is being developed through an open process, allowing for a robust technical basis that aligns with business interests. By relying on practices developed, managed, and updated by industry, the Framework will evolve with technological advances and will align with business needs.

The Framework provides a uniform guide for developing robust cybersecurity programs for organizations. This includes industry-driven standards, best practices and implementation measures to manage cybersecurity risks to information technology and operational technology.

The Framework provides a common structure for managing cybersecurity risk, and will help you identify and understand your organization's dependencies with its

business partners, vendors, and suppliers. In doing so, it will allow you to coordinate cybersecurity risk within your industry and sector for the delivery of critical infrastructure services.

Unique missions, threats, vulnerabilities, and risk tolerances may require different risk management strategies. One organization's decisions on how to manage cybersecurity risk may differ from another. The Framework is intended to help each organization manage cybersecurity risks while maintaining flexibility and the ability to meet business needs. As a result, the Framework is not designed to replace existing processes. If an organization does not have an existing risk management process for cybersecurity, the Framework provides the tools to build one. By implementing the Framework, an organization can take steps to improve the resilience of its services while protecting data and intellectual property. This methodology is designed to instill trust from the sector and partners and protects the organization's brand and reputation.

Using the Framework

The Framework places cybersecurity activities into five functions: identify, protect, detect, respond, and recover. Your organization should implement capabilities in each of these areas.

Implementing the Framework will help you align and communicate your cybersecurity risk posture with your partners and help communicate expectations for managing cybersecurity risk consistent with your business needs. As the Framework is implemented throughout critical infrastructure, lessons learned and improvements will be integrated, to ensure it is a dynamic and relevant framework.

The repeated cybersecurity intrusions into the nation's critical infrastructure have demonstrated the need for a stronger approach to manage cybersecurity. Every organization involved in critical infrastructure services is invited to actively participate in the development, validation, and implementation of the Cybersecurity Framework.