FACT SHEET:
Cybersecurity Framework Version 1.1

Background:

The Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") is a voluntary framework developed through a collaborative process by industry, academia, and government stakeholders. NIST continues, as directed by the Cybersecurity Enhancement Act of 2014, to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices. It is designed to be relevant for every size, sector, and type of organization.

The Framework provides an approach to prioritize cybersecurity resources, make risk decisions, and take action to reduce risk. It enhances cybersecurity communication within an organization and with other organizations (such as partners, suppliers, regulators, and auditors) and helps organizations identify, manage, and assess cybersecurity risks.

The Cybersecurity Framework consists of 3 components:

1. **The Core**: provides an easy-to-understand set of desired cybersecurity outcomes.
2. **Profiles:** portrays organizations' unique requirements, objectives, risk appetite, and resources.
3. **Implementation Tiers**: indicates how an organization manages cybersecurity risks.

Summary of Cybersecurity Framework Version 1.1 Updates:

The v1.1 update process began in 2015 and is the product of significant stakeholder discourse (including 200+ written comments for the two draft publications and dialog with 1,200+ participants at the 2016 and 2017 annual workshops). The engagement model that we used for Framework v1.0—which garnered high praise from the cybersecurity community—continued during the development of v1.1. **The document has now evolved to be even more informative, useful, and inclusive for all kinds of organizations.**

Key points about v1.1:

- Refined for clarity, it's fully compatible with v1.0 and remains flexible, voluntary, and cost-effective
- Declares applicability for "technology," which is minimally composed of Information Technology, operational technology, cyber-physical systems, and Internet of Things
- Clarifies utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements
- Enhances guidance for applying the Cybersecurity Framework to supply chain risk management
- Summarizes the relevance and utility of Cybersecurity Framework measurement for organizational self-assessment
- Better accounts for authorization, authentication, and identity proofing

Resources:

- **Cybersecurity Framework v1.1 publication**: https://www.nist.gov/framework
- **Cybersecurity Framework website**: https://www.nist.gov/cyberframework
- **Follow us on Twitter**: @NISTcyber

Document last updated on 3/10/2018