NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

As directed by Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," the National Institute of Standards and Technology (NIST) led the development of a voluntary framework–based on existing standards, guidelines, and practices – for improving cybersecurity risk management within critical infrastructure. NIST developed the Framework through a year-long process by collaborating with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders. The process included a public request for information, five national workshops, and numerous meetings, webinars, and informal feedback sessions.

These interactions ensured international input and feedback regarding the approach for developing the Framework, and informed the drafting, shaping, and revision of initial versions of the Framework and supporting material.

Given the range of entities that comprise the critical infrastructure, the Framework is designed to be relevant for organizations of nearly every size and composition. The Framework is also designed to be applicable throughout an entire organization – from the senior executives who oversee an organization to the officials and staff responsible for managing critical infrastructure systems and information technology resources.

Framework Description

The Framework is designed and intended:

- To be an adaptable, flexible, and scalable tool for voluntary use;
- To assist in identifying, assessing, and managing cybersecurity risks;
- To complement current regulatory authorities;
- To promote technological innovation;
- To raise awareness of the challenges of cybersecurity and the means for understanding and managing the related risks;
- To be consistent with voluntary international standards.

Framework Core

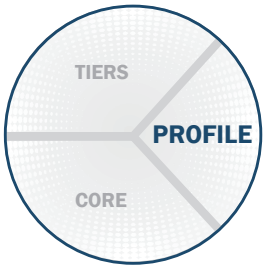
The Framework Core consists of five Functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these Functions provide a high-level, strategic view of the organization's cybersecurity risk management lifecycle. While they do not replace a risk management process, these five high-level Functions help an organization answer fundamental questions, including "How are we doing?"

ID	**Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PR	**Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DE	**Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RS	**Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
RC	**Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

NIST CYBERSECURITY FRAMEWORK
Managing Cybersecurity Risk

Framework Implementation Tiers

Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. During the Tier selection process, an organization considers its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. These Tiers reflect a progression from informal, reactive implementations to approaches that are agile and threat-informed.



Framework Implementation Profiles

A Framework Profile represents the outcomes that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Most importantly, profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the desired state). Organizations can use that information to develop action plans to strengthen existing cybersecurity practices and reduce cybersecurity risk. Organizations may also find that they are overinvesting to achieve certain outcomes and can reprioritize resources to strengthen other cybersecurity practices. Profiles can be used to communicate a particular security posture to another organization. This type of interaction can be used to drive requirements at early stages of the acquisition process.

Next Steps

By using the Framework as a common language to communicate cybersecurity activities and outcomes, the community can continuously improve the process of identifying, assessing, and managing cybersecurity risk. NIST is committed to continuing the discussion surrounding the use and governance of the Framework. Organizations are encouraged to use the Framework to augment their own cybersecurity risk management practices and communicate their findings. NIST encourages industry to discuss the tools, practices, and lessons learned within the community to facilitate the evolution of the Framework. NIST will work on version 2.0 of the Framework with industry and will continue the process of public discourse through a workshop.

Helpful Links:

Framework: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
Roadmap: http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf
DHS C3VP: http://www.us-cert.gov/ccubedvp