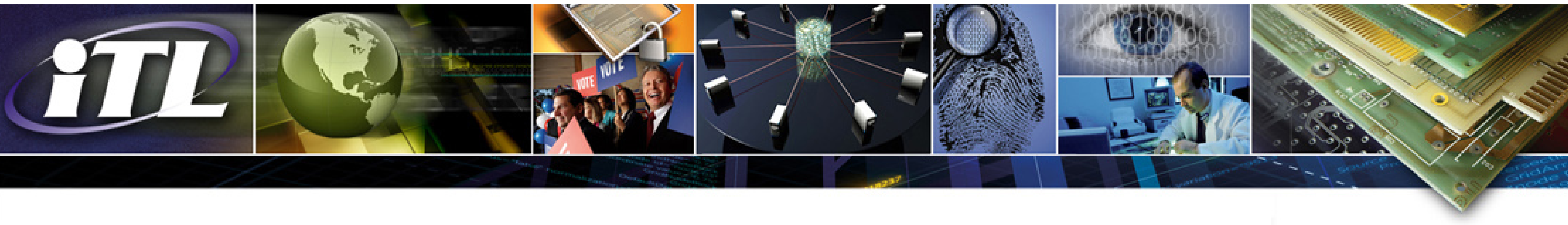


ITL BULLETIN FOR FEBRUARY 2014

FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

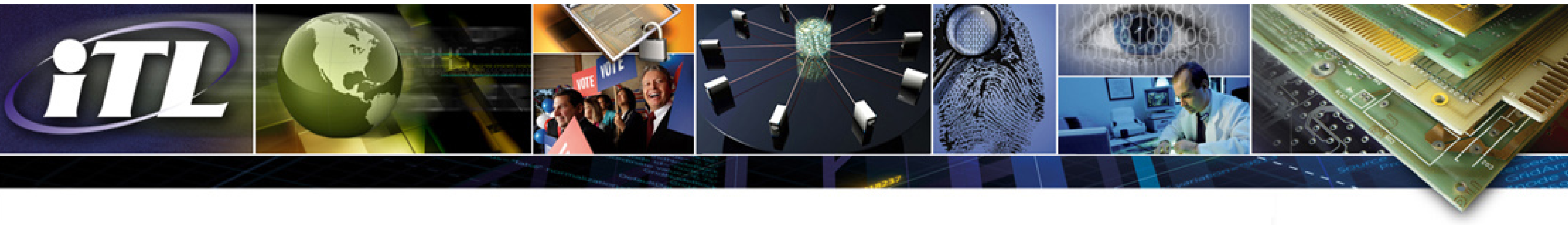
Kevin Stine, Kim Quill, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Recognizing that the national and economic security of the United States depends on the resilience of critical infrastructure, President Obama issued Executive Order (EO) 13636*, Improving Critical Infrastructure Cybersecurity*, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cybersecurity risks.

In support of this directive, the Computer Security Division (CSD) of NIST's Information Technology Laboratory (ITL) led the development of the Cybersecurity Framework. The Cybersecurity Framework provides a prioritized, flexible, repeatable, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties. To enable technical innovation and account for organizational differences, the Framework does not prescribe particular technological solutions or specifications.

NIST worked with a diverse stakeholder community to develop the Framework through an open and public process. The NIST Framework team:

- Issued a request for information (RFI) in the *Federal Register* in February 2013, to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework. It requested comments regarding benefits and limitations of current risk management practices; regulations; current practices; methodologies in use by critical infrastructure; and privacy and civil liberties considerations.
- Conducted five open workshops to provide the public with additional opportunities to provide input. These workshops were hosted at the Department of Commerce in Washington, D.C. (April 2013); Carnegie Mellon University in Pittsburgh, PA (May 2013); the University of California, San Diego, CA (July 2013); the University of Texas at Dallas, TX (September 2013); and the North Carolina State University in Raleigh, NC (November 2013).
- Developed a Preliminary Cybersecurity Framework for official public review and comment. More than 200 reviewers submitted written responses, resulting in nearly 2,500 specific comments. CSD considered each of these comments as it developed the Cybersecurity Framework that was published on February 13, 2014.

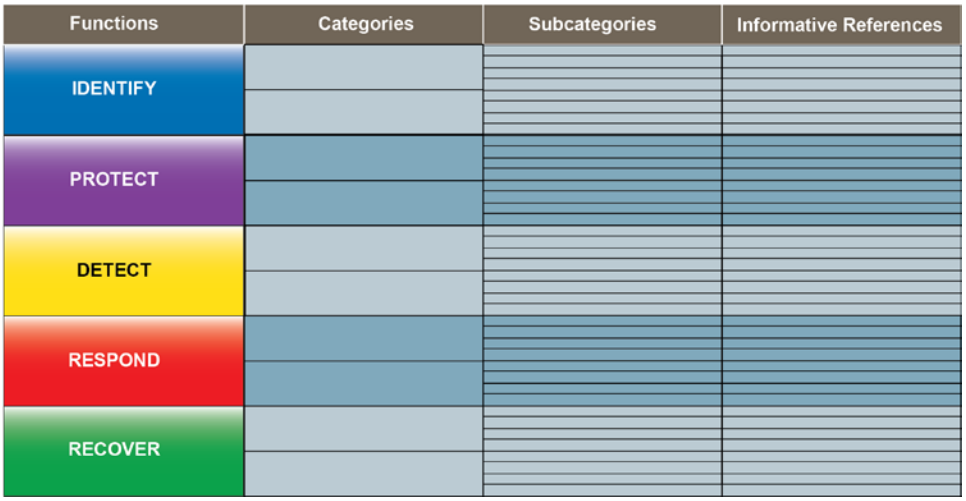


The Framework is risk-based, and is composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework provides a common taxonomy and mechanism, based on existing standards, guidelines, and practices, for organizations to:

- 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; and
- Communicate among internal and external stakeholders about cybersecurity risk.

The Framework Core

The Framework Core, illustrated in Figure 1, is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1 - Framework Core Structure

The Core elements in Figure 1 operate as follows:

- **Functions** organize basic cybersecurity activities at their highest level. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Example categories include “Asset Management,” “Access Control,” and “Mitigation.”
- **Subcategories** further subdivide a Category into specific outcomes of technical and/or management activities. They provide a set of results that help support achievement of the outcomes in each Category. The set of Subcategories is not intended to be an exhaustive list, and organizations may tailor these as needed.
- **Informative References** are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each Subcategory. Informative References are intended to be illustrative and represent the set of cross-sector references most frequently cited during the Framework development process.

The Framework Profile

The Framework Profile (“Profile”) represents the outcomes based on business needs 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. 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 “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization’s risks. That Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

The Framework Implementation Tiers

The Framework Implementation Tiers (“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 should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization’s cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

Additional Resources

The Cybersecurity Framework is available at http://www.nist.gov/cyberframework.

Information about NIST’s information security programs, standards, guidelines, and related publications is available from the Computer Security Resource Center at http://csrc.nist.gov.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.