ITL BULLETIN FOR MARCH 2013

NIST TO DEVELOP A CYBERSECURITY FRAMEWORK TO PROTECT CRITICAL INFRASTRUCTURE

Elizabeth Lennon, Editor
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The reliability and trustworthiness of our nation's critical infrastructure is vital to the economic and national security of the United States. Under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," the President has directed NIST to develop a voluntary framework for reducing cyber risks to our nation's critical infrastructure. The Cybersecurity Framework will consist of standards, methodologies, and procedures that promote the protection of information systems supporting crucial infrastructure operations. It will promote the wide adoption of best practices to increase cybersecurity across all sectors and industry types. The flexible and cost-effective approach of the Framework will assist owners and operators of critical infrastructure in managing cybersecurity risk while ensuring business confidentiality and individual privacy.

Working with stakeholders in government, industry, and academia, NIST's Information Technology Laboratory has initiated the development of the Framework by conducting a comprehensive review of the current cybersecurity landscape through a Request for Information (RFI). Published in the *Federal Register* of February 26, 2013, the RFI requests information to identify, refine, and guide the many interrelated challenges and efforts needed to draft the Framework. As always, NIST will engage with and seek input from stakeholders through an open public review and comment process, workshops, and other means of engagement.

We invite you to attend the first Cybersecurity Framework Workshop on Wednesday, April 3, 2013, at NIST. For more information and to register, go to the workshop website. The workshop is free of charge, but registration is required.

We also invite your input and comments to the RFI. Online submissions in electronic form may be sent to cyberframework@nist.gov. Comments are due by **April 8, 2013.** Complete information is available in the Federal Register notice.

With input from government and industry stakeholders, our goal is to develop a substantive and comprehensive Cybersecurity Framework to protect our nation's critical infrastructure.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email 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.