ITL BULLETIN FOR NOVEMBER 2013

ITL RELEASES PRELIMINARY CYBERSECURITY FRAMEWORK

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently released a Preliminary Cybersecurity Framework for public review and comment. ITL developed the framework based on information gathered from stakeholders over the past six months including a Request for Information in the *Federal Register* dated February 26, 2013, and a series of four public workshops held at various locations throughout the United States. The purpose of the framework is to strengthen the resilience of the nation's critical infrastructure upon which the health, security, and sound economy of our country relies.

NIST is developing the framework under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which calls for a voluntary cybersecurity framework that provides for a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk. Consisting of standards, guidelines, and methodologies that promote the protection of information systems supporting critical infrastructure operations, the framework will facilitate 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.

We invite you to attend the fifth Cybersecurity Framework Workshop on November 14-15, 2013, at North Carolina State University in Raleigh, North Carolina. At this workshop, ITL will continue discussions on the implementation and future governance of the Cybersecurity Framework. For more information and to register, go to the workshop website. The workshop is free of charge, but registration is required.

As announced in the Federal Register notice of October 29, 2013, we are seeking your input and comments on the Preliminary Cybersecurity Framework. Electronic comments should be submitted in Microsoft Word or Excel formats to: csfcomments@nist.gov, with the Subject line: Preliminary Cybersecurity Framework Comments. Written comments concerning the preliminary Framework may be sent to: Information Technology Laboratory, ATTN: Adam Sedgewick, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930. All comments will be posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or business information). **Comments are due by December 13, 2013**. Complete information is available in the Federal Register notice.

With continued 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