Information Assurance Advisory, LLC
301 McCullough Drive, 4th Floor, Charlotte, NC 28262-3310
Phone: 704-236-2385 Fax: 704-909-2701
www.iaadvisory.com

Comments in response to Federal Register Docket Number 130208119-3119-01, "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Information Assurance Advisory, LLC is pleased to offer the comments below in response to the NIST Request for Information (RFI). The comments below are based on my personal experiences and responsibilities for addressing and managing information technology security risks in both governmental and private sector organizations.

The list of questions provided in NIST RFI focused on standards, guidelines and practices and the applicability of existing publications along with their usage within various organizations. The supplementary information section of the RFI stated the Framework will build on several ongoing work and related products. The current products referenced provide limited guidance on an essential aspect that is necessary to achieve the goals stated for the Framework.

To assure standards, guidelines, practices and controls are effectively risk managed, resourced, implemented properly, and monitored, an organization or corporation must have a compressive risk management and information technology governance structure implemented with mature organizational management processes. Efforts, such as those found in COBIT 5 and ITIL® provide valuable process and guidance.

Additionally, complex information technology implementations and operations, such as those of critical infrastructures, require a disciplined development and agreement on the enterprise architectures (EA) within organizations and corporations. The efforts of The Open Group, which developed the The Open Group Architectural Framework (TOGAF) should be examined. The TOGAF describes the EA framework. The NIST Smart Grid effort, as an example, required a common architectural understandings to best align security practices and controls based on a risk assessment.

The Department of Commerce has stated, "The cyber threat to critical infrastructure is growing and represents one of the most serious national security challenges that the United States must confront." Others within the U.S. government have echoed similar warnings. This threat includes exploitation efforts by nation states and produces a conundrum for commercial owners and operators of critical infrastructures. Security practices and controls to operate a business in a competitive marketplace are generally insufficient against a well-resourced nation state. The Framework must address in its risk management, standards and guidelines how to address that likely gap. It may not be possible to describe the procedures or processes to address this gap in public documents; as those details would be of significant value to the perpetrator of the threat. If so, a corresponding classified Framework will be required and should be part of NIST consultative processes considerations.

We encourage NIST's continued work in configuration management and automation and expect those related NIST 800 series efforts will be of significant value and should be an essential element addressed in the Framework.

Roger M. Callahan

Roger M. Callahan
Managing Director

ITIL® is a registered trademark of the U.K. Cabinet Office