8 April 2013

Via cyberframework@nist.gov

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

ASIS International is the world's preeminent association of security professionals, with 38,000 members around the globe, nearly three-quarters of those in the United States. The majority of our members are managers responsible for planning, conducting, and assessing security operations in critical infrastructures, including those that are owned or operated by the private sector.

We are taking the opportunity to respond to the National Institute of Standards and Technology (NIST) notice, "Developing a Framework to Improve Critical Infrastructure Cybersecurity." NIST is no stranger to ASIS. As an American National Standards Institute (ANSI)-accredited standards development organization, ASIS knows and appreciates the role that NIST plays in scientifically working toward improved American productivity and competitiveness.

We recognize and appreciate NIST's stated intention that the Framework will: be consensus-based; not prescribe particular technologies or specifications; seek to foster widespread adoption; and seek to find commonality among sectors.

We wish to highlight several principles of particular importance to our members,

- The primary responsibility for development of the Framework should be with the owners and operators of critical infrastructures. The Framework should complement, not replace, existing regulatory standards pertaining to cybersecurity.

- Methods to be used for information-sharing and associated rules for collection need to be specified. Methods for protecting information also need to be specified.

- Incentives for information-sharing (including, but not limited to, protections relative to liability, FOIA Requests and regulatory use of collection information) need to be clearly spelled out.

- It is especially important—given the nature of cybersecurity threats—that a mechanism to ensure constant and swift technological refreshing of the Framework is maintained to avoid outdated rules, processes and tools.

- Section 10 is worrisome because agencies are being required to report on “any additional authority” required in the Framework. A consensus based upon the most modern situational awareness and security intelligence methodologies would be more effective than a compliance structure.

We look forward to working with NIST in development of the Framework. We have in our membership security leaders from every industry who want to help our federal government and their fellow security professionals in this vital work.

Sincerely,

/s/

Jack Lichtenstein
Vice President, Government Affairs & Public Policy
ASIS International
1625 Prince Street
Alexandria, VA 22314