INSA INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

The Intelligence and National Security Alliance (INSA) submits the attached comments in response to the NIST document, *"Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework"* released on October 23, 2013. We hope our comments encourage discussions around incorporating the concepts of cyber intelligence and insider threats into the Cybersecurity Framework.

INSA is a non-profit, non-partisan professional organization established in 2005 to improve our nation's security through an alliance of intelligence and national security leaders from government, industry, and academia. Evolved from the Security Affairs Support Association (SASA) which was established in 1986, INSA members collaborate to provide practical solutions and insight to key policy and industry issues affecting US intelligence and national security.

The INSA Cyber Council is a group of current and former executives from the public, private, and academic sectors with expertise in variety of cyber areas including security. The Council engages government, industry, and academia in pursuit of innovative solutions and thought leadership that will improve existing cyber security policies, practices, and organization. Recognizing the need for a transformative, intelligence-driven approach to cybersecurity, the Council formed its Cyber Intelligence Task Force to explore the relevance of intelligence methodologies with regard to analyzing and understanding cyber threats and provide thoughts on how to develop this discipline in the cyber domain. In conjunction, the Cyber Council formed its Cyber Insider Threat Task Force to examine best practices regarding internal cyber security measures and offer ways the public, private, and academic sectors can improve their cyber security policies and practices to protect against insider threats.

The INSA Cyber Council applauds the work that NIST is doing to improve the cybersecurity posture of the nation's critical infrastructure. The NIST Framework provides a comprehensive outline of the essential elements of cybersecurity, not only for critical infrastructure but for other types of organizations as well. The Framework provides an effective approach to risk management, perimeter defense, network defense, response, and recovery.

We believe cyber intelligence is foundational to a full understanding of the cybersecurity enterprise and its vulnerabilities. Critical infrastructure organizations need to operate within the context of a well thought out and dynamic defense, informed by intelligence at the strategic, operational, and tactical levels, which addresses awareness of actual threats and prepares for potential threats. Reactive defense postures are no longer sufficient for an adequate risk management strategy. Cybersecurity planning and operations must be intelligence-driven to:

- Transform the cybersecurity posture from reactive to proactive.
- Permit shift from static perimeter defenses to meaningful, dynamic defensive operations.
- Enable an adaptive cybersecurity posture based on a continuous assessment of the threat/risk environment and its implications for an organization's enterprise security activity.

Risk assessment is an important part of intelligence-driven cybersecurity, but the function of "risk assessment" does not adequately describe the comprehensive function of the concept of cyber intelligence.

INSA's comments are attached in template format as requested by NIST. The INSA white papers, *Operational Levels of Cyber Intelligence* and *A Preliminary Examination of Insider Threat programs in the U.S. Private Sector* are attached for context.

The INSA Cyber Council would welcome the opportunity for further discussion with NIST on this important issue. If a presentation or discussion with the INSA Cyber Council is of interest please contact Chuck Alsup, Vice President of Policy at the Intelligence and National Security Alliance. CAlsup@insaonline.org, (703) 224-4672 .

Charles W. Alsup
Vice President for Policy
Intelligence and National Security Alliance