Arizona Cyber Threat Response Alliance

c/o AZ DPS, 2102 Encanto Blvd, MD 3900, Phoenix, AZ 85009
TEL 623-551-1526 • FAX 623-551-4221

December 12, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
csfcomments@nist.gov

Subject: Preliminary Cybersecurity Framework

The Arizona Cyber Threat Response Alliance (ACTRA) appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST) Preliminary Framework to Improve Critical Infrastructure Cybersecurity as described by the February 2013 Presidential Executive Order 13686.

ACTRA is a non-profit, volunteer-driven organization that serves as a hu for collaborative cyber information-sharing in a neutral environment of trust where Arizona partners from industry, academia, law enforcement and intelligence come together to leverage cross-sector resources and respond to emerging cyber threats to Arizona's Critical Infrastructure and Key Resources (CI/KR).

ACTRA appreciates and commends NIST's thorough, open and transparent process to engage all stakeholders in the process of developing this essential national resource. Active involvement of industry and incorporating their input helps ensure the Framework both strengthens our critical infrastructure security and supports vital innovation in continually improving that security.

Dangerous cyberthreats to CI/KR are escalating at an extraordinary rate. Countering these increasingly sophisticated threats necessitates an equally sophisticated response, one that requires the cooperative efforts of government, industry and NGO stakeholders working together. Effective cooperation is only possible, though, with a central unifying structure available to help harmonize all efforts, and a voluntary national cybersecurity Framework can be such structure. Carefully crafted, it can deliver valuable guidance, encourage best practices, enable innovation, and in particular, provide common vocabulary for information sharing among all stakeholders, a critical component for a coordinated cyber defense.

Based o the preliminary draft provided for comments, we believe NIST's Framework can meet these goals and provide a solid foundation for all CI/KR organizations to help build new or bolster their existing cybersecurity programs. The proposed Framework incorporates number of best practices and industry-accepted standards into a flexible and scalable framework that any organization can easily apply to its own environment.

Implementing effective cyber security programs aligned with the central structure is equally important, but must originate at the local level, as only there can security risks be correctly assessed and mitigated. Locally implementing a cybersecurity program from a national structure, however, is not always an easily identifiable path. To address this problem, ACTRA intends to help Arizona CI/KR organizations understand the Framework and its role in an organization's cybersecurity. We believe we are uniquely situated to help translate the ambitious national goals captured in the Framework into concrete actions at the state, local, and tribal level.

To aid all local efforts to align with the Framework, as development of the Framework continues towards its initial release in Q1 2014 we recommend NIST and its partners address these remaining issues:

Governance – NIST has made clear the Framework is a living document and will continue to evolve along with the cybersecurity landscape. To best facilitate that evolution, we recommend NIST continue driving towards a model of industry governance of the Framework starting in 2015. This will ensure the Framework not only evolves, but does so well-aligned with the latest cybersecurity advancements and needs of CI/KR industries and organizations.

Small and Medium Business (SMB) support – While a small or medium business may not be at the epicenter of a catastrophic event, recent examples worldwide have demonstrated that SMBs are critical to recovering from such events. We recommend NIST continue to strengthen the Framework's ability to address the unique cybersecurity needs of many SMBs. Additionally, there should be a permanent, specific touchpoint within the Framework governance program that liaisons with and supports the SMB community directly.

Education an Training – Considerable information and assistance is needed to understand and adopt any cybersecurity framework. NIST has provided much supporting material, but it will also require specific educational materials for the Framework to be completely successful, aimed at both the private sector as well as state, local, and tribal governments. We recommend NIST facilitate the production of materials suitable to train security professionals on Framework applications, as well as materials that educate all interested citizens on the Framework and its benefits.

Thank you again for the opportunity to provide comment o the Preliminary Cybersecurity Framework. Now more than ever, we must leverage the full expertise of both the federal government and the private sector to solve the important and complex problem of better securing our critical infrastructure in ways that harnesses innovation to address the needs of governments, businesses, and citizens. As part of that effort, ACTRA will continue to assess and leverage the Framework, as it develops and evolves, for the benefit of the Arizona CI/KR environment.

Best Regards,

Frank J. Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance, Inc.