Missouri Credit Union Association

April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Don Cohenour - Comments on Developing a Framework to Improve "Critical Infrastructure" Cybersecurity

Dear Ms. Honeycutt:

On behalf of its 1.3 million credit union members, the Missouri Credit Union Association (MCUA) appreciates the opportunity to respond to the National Institute for Standards and Technology's (NIST's) request for information on the coordination of a "critical infrastructure" cybersecurity standards framework (framework). The NIST is gathering information that will help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the U.S. cybersecurity framework. This request for information provides a positive, initial step on the coordination of a framework to implement the White House Executive Order (EO) and Presidential Policy Directive on cybersecurity issued in February 2013.

MCUA agrees with NIST that the framework should "be compatible with existing regulatory authorities and regulations" which will promote innovation and "not prescribe particular technological solutions or specifications." As NIST Undersecretary Dr. Patrick D. Gallagher noted in his written testimony for the March 2013 Senate hearing on cybersecurity, private entities are already supporting critical infrastructure and "should not be diverted from those efforts through new requirements."

Under the EO, the Secretary, in coordination with sector-specific agencies, will establish a voluntary program to support the adoption of the cybersecurity framework by "critical infrastructure" entities, as well as other interested entities. NIST should coordinate with stakeholders to ensure that any voluntary "critical infrastructure" initiatives remain voluntary, and not impose additional requirements for other entities that are not part of the program.

In addition, the cybersecurity framework should provide protections on business confidentiality, individual privacy and civil liberties. NIST should coordinate with stakeholders on these important issues, in addition to data and information security goals. Further, NIST and other government entities should focus on cybersecurity education and providing access to timely information, so public and private stakeholders are informed on cyber threats and can take steps to protect their interests.

Currently, credit unions are subject to data security requirements from a plethora of agencies and laws such as rules from the National Credit Union Administration (NCUA) and Federal Financial Institution Examination Council (FFIEC). NCUA regulates and implements data security requirements and standards for credit unions. These data security requirements and standards include the federal laws of the GrammLeach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and Right to Financial Privacy Act (RFPA). Other standards apply to financial institutions, such as the Payment Card Industry Data Security Standards (PCI-DSS) on payments card data security. Also, NCUA has published agency Letters to Credit Unions, Regulatory Alerts, Legal Opinion Letters, and other guidance in response to data security, cybersecurity, and consumer protection laws.

In summary, thank you for the opportunity to respond to the NIST's request for information regarding cybersecurity. We will be happy to respond to any questions regarding these comments.

Sincerely,

Don Cohenour
Interim President