December 13, 2013

National Institute of Standards and Technology
Information Technology Labratory
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments

Dear Adam Sedgewick,

This comment letter represents the views of the League of Southeastern Credit Unions & Affiliates (LSCU) regarding the National Institute of Standards and Technology's (NIST's) request for comment on the preliminary framework developed in response to the White House Executive Order (EO) and Presidential Directive (PPD) on cybersecurity. By way of background, LSCU is a credit union advocacy organization, representing approximately 285 state and federal credit unions, which serve about 6 million members.

LSCU supports NIST's efforts to develop a framework that provides for a flexible, performance-based, cost-effective and prioritized "infrastructure" that aids in managing cybersecurity risk while at the same time protects the confidentiality of businesses, privacy of individuals and civil liberties of all. We urge NIST to continue to seek balance in these areas and we view the coordination of public and private sectors on cybersecurity as the key component to that end.

We found the Preliminary Cybersecurity Framework as adequate for defining the outcomes that strengthen cybersecurity and support business objectives. Further the information available to executives and supervisory boards were beneficial in promoting an understanding of the risks present and how institutions should go about attempting to lessen the risk.

The Preliminary Framework, while clear in its stated goal, does not sufficiently provide adequate data that would indicate if this will be a cost-effective implementation.

Presently there are so many resources in play that it is not clear whether there is enough guidance available to ensure a cost-effective implementation. Standardizing the information or recommendations would be most helpful and would serve to simplify any implementation guidelines. As is often the case with highly technical implementations, smaller credit unions will likely feel the burden of meeting the required standards far more than those institutions with greater resources.

Credit unions that make up our membership are already subject to omnibus cybersecurity and data security requirements. These requirements include those present in the Gramm-Leach-Bliley Act (GLBA) and other data security laws, regulations, and standards from governmental and supervisory agencies such as the

Federal Financial Institutions Examination Council (FFIEC) and the National Credit Union Administration (NCUA). As you are aware, the FFIEC prescribes uniform principles, standards, and report forms for the federal examination of financial institutions, including our member credit unions.

To avoid an implementation or rollout that is disruptive and counterproductive, any new framework must be compatible with current regulatory guidelines and regulations. NIST Undersecretary Dr. Patrick D. Gallagher noted in his written testimony to the Senate in a March 2013 Senate hearing on cybersecurity, private entities are already supporting critical infrastructure and "should not be diverted from those efforts through new requirements." We agree. To do so would be unnecessary and immeasurably set back the effort to develop critical framework.

NCUA is responsible for regulating and implementing data security requirements and standards for credit unions. These data security requirements and standards are far reaching and include federal laws such as the Gramm-Leach Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Right to Financial Privacy Act (RFPA), as well as a myriad of state laws and other rules.

In addition, credit unions are required to adhere to data security requirements found under § 501(b) of the Gramm-Leach Bliley Act (GLBA) and part 748 of the NCUA's own regulations. Credit unions are required to have in place comprehensive data security programs designed to provide safeguards for member and consumer records and information. The aim of these programs is to ensure the security and confidentiality of financial information and data; guard against malicious threats or hazards to the security and integrity of credit union records; and prevent unauthorized access to or illegal use of c credit union records or information that could result in substantial harm to any member or consumer.

We believe the current requirements enable credit unions to defend themselves against those that would seek to damage the institution or its members and a review of the preliminary framework leads us to believe that credit unions could satisfactorily incorporate threat information as well.

We applaud the NIST's efforts to help secure the nations "critical infrastructure" through the development of the proposed cybersecurity standards framework. To assist that effort, our league and our member credit unions will continue to emphasize the use of current data security and cybersecurity rules such as those from the NCUA, FFIEC, and GLBA. We also intend to continue our efforts to ensure that any new cybersecurity framework will recognize current data security standards that are now requirements for our affiliated credit unions. New rules and regulations will not improve the environment if they are simply layered over previous data security efforts so we strongly urge you to avoid this result at all costs.

Thank you for the opportunity to comment on the Preliminary CyberSecurity Framework issue and for considering our views.

Sincerely,

Scott Morris
Compliance Director
League InfoSight

cc: CCUL