Developing a Framework to Improve Critical Infrastructure Cyber Security Mark Ritchie, Secretary of State, Minnesota

As Secretary of State of Minnesota, I appreciate the opportunity to provide comments in response to the Request for Information (RFI) issued by the National Institute of Standards and Technology (NIST) for the creation of a Framework to Improve Critical Infrastructure Cyber Security in support of Executive Order 13636 issued by President Obama.

As Secretary of State I am the chief elections officer in Minnesota and work closely with county and local election officials to administer elections. I also chair a State Canvassing Board, which certifies the results of elections.

"Critical infrastructure" has the meaning given the term in 42 U.S.C. 5195c(e), "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." While the administration of our federal and local elections is fundamentally and necessarily the responsibility of State governments, U.S. security is inexorably dependent on the sound functioning of our election systems.

Submitted by Secretary of State Mark Ritchie

In the last two decades, our election systems have become almost entirely reliant on computer technology, introducing new risks and vulnerabilities into the election process. More recently, we have seen a rapidly increased use of the Internet in the administration of elections. While some of this has been implemented with serious attention to the potential of cyber-threats much of it has not. For example, some jurisdictions have authorized voting to take place over the Internet, thereby exposing the election process to very serious threats of denial of service attacks and other cyber dangers.

As a vital component in our nation's critical infrastructure, the expanding use of the Internet in the administration of elections certainly warrants the assistance, support and resources of the relevant federal government's cyber security agencies. Yet, to date, contemplation of cyber vulnerabilities of U.S. election systems and technology has been noticeably absent from discussions or policy addressing cyber security challenges facing our critical infrastructure.

NIST's RFI stated that the goals of the Framework development process will include "(ii) to specify high-priority gaps for which new or revised standards are needed; and (iii) to collaboratively develop action plans by which these gaps can be addressed." I would like to identify the use of online election procedures and systems as a high priority area within the critical infrastructure which has been overlooked. Because no cyber security standards currently exist for this area, NIST will need to collaboratively develop an action plan to address this gap.

While State governments must deal with the cyber threats that exist, our expertise and resources cannot compare to those of the federal government in the area of cyber security. As a State election officer, I encourage NIST to share its experience, expertise and recommendations regarding the cyber threat to the election system so that we may all address the security threats that exist.

While election administration will benefit from many standard computer hygiene and security practices, it also has many unique characteristics which make it unlike other processes. Because the voter submits

a secret ballot, it is much more difficult to detect tampering or intrusion compared to online commerce or banking. Moreover, while banks and credit card companies can define and absorb an "acceptable" level of fraud, elections can be (and in my state, have been!) decided by less than a few hundred votes. As chief elections officer, I cannot tolerate any level of tampering or hacking.

For this reason, I strongly support NIST's commitment to engage state and local governments, organizations, agencies and stakeholders in the development of guidance, best practices and security recommendations for the protection of our election system's cyber security. I urge NIST to work collaboratively with election officials in adapting cyber security standards to the field of election administration.

Thank you for the opportunity to submit comments on this critically important issue. I hope to work with NIST on developing guidance, best practices and security recommendations in election administration.

Mark Ritchie, Minnesota Secretary of State