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

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

The Accredited Standards Committee X9, Inc. ("X9") – Financial Industry Standards submits this response to the Request for Information ("RFI") seeking information on "standards, methodologies, procedures, and processes that align policy, business and technological approaches to address cyber risks." 78 Fed. Reg. 13024 (February 26, 2013). X9 is the ANSI-accredited standards development organization in the United States for financial services standards. X9 standards are voluntary, consensus public standards covering all core banking functions, as well as retail payments, corporate financial areas, and securities. X9 membership includes representatives of all major stakeholders in the financial services industry, from banks, banking associations, branded card companies, card transaction processors, merchants, to suppliers/vendors and government agencies.

Background

NIST, under the authority of The Department of Commerce, is seeking the above information to develop a "Cybersecurity Framework" to reduce risks to critical infrastructure. The substance of the RFI is to reinforce the role of standards-based Framework(s) that will help provide some of the measures necessary to understand the effectiveness of critical infrastructure protection, and track changes over time. The RFI is looking for current adoption rates and related information for particular standards, guidelines, best practices, and frameworks to determine applicability though out the critical infrastructure sectors.

The RFI poses numerous questions, some of which are relevant to the banking security standards work. Accordingly, X9 provides answers only as it relates to its body of work .

Financial Services Standards Review

The RFI requests information on the use of frameworks,standards, guidelines, and best practices (see p. 13027). The United States Financial Community (and its international counterparties) has been actively developing, implementing and using industry developed (among others) standards for more than 30 years. Standards for banking have included a broad scope of what could be defined through banking services, such as Payments security, checks, credit/debit transactions, securities transactions, codes, Mobile, Cloud, and other services, all of which are considered critical infrastructure in today's global economy. All one needs to know about the criticality of the US payment infrastructure can be summarized by the impacts caused by the physical interruption of the flow of paper checks throughout the country when flights were grounded on 9-11.

Attached is a non-exhaustive relational diagram reflecting many of the existing standards related to data and information security standards, which have been developed by X9 through its Subcommittee on Data Security, along with an explanation of each standard. It should be noted that NIST is a member of this Subcommittee and has participated in the development of some of these standards (see further discussion below). X9 also wishes to point out that many of these US national standards are adopted as ISO standards and implemented globally as banking/financial services are global and interoperable.

As banking and financial services transitioned from paper to electronic banking and financial services transactions beginning in the 1970's , so did the need and requirements for data security across both forms. Many standards were developed around a specific industry requirement or a new service provision to banking consumers and customers; the PIN, personal identification number, standard is an excellent example of this. Additionally, these new requirements and services quickly pushed the financial services industry to protect not only transaction services provided nationally within the U.S., but also to secure international transaction services. Because of this international usage, banking was among the first industries to require strong and effective encryption and its global export within payments-related hardware. Over time, the financial services industry has developed a long history of working with NIST, NSA and other federal agencies to gain these permissions, and in the process those agencies became active participants in X9's data security standards development process. This over-arching standards activity continues today as X9 turns its focus to among other services - mobile banking and cloud computing data security standards for the financial services industry.

The attached illustration shows a view of Financial Services Security categorized into four entities. An initial entity is a methodology to define security through layers. Not only do these layers provide appropriate delineation for security approaches in banking/financial services, but these layers can be applied to other markets beyond banking, and the generic terminology for

each layer is such that meanings can be extracted by a broad readership. We note that "NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry"(see first paragraph in Specific Industry Practices, p. 13027). For example, the Authentication layer can be associated with individual (in banking the customer) identity, accessing rights, and mechanisms that can be implemented for a measured risk; Identity can be considered global in usage; whereas Authorization can be seen as local and other security mechanisms that can be applied across a host of applications.

The continuum of these layers provides a broad picture of where security can be focused. Combinations of these security layers are seen in financial services applications. In continuing with the other entities within the illustration, a Security Function has been defined that correlates and further identifies specific functions which can be associated with each of the security layers. The X9 security standards have a close parallel with these functions and offer X9 a visual representation of where potential new standards may be needed. The list of X9 security standards included in the illustration has a matching color correlation with the security layers and security functions. The last two entities provide a summation of what could be considered: the "business of security", and the "mapping security across banking services." There are regulatory, legal, contractual and other business considerations as security is applied, and for a comprehensive security framework to be effective, it must be able to map to the available banking services. The attachment becomes a snapshot in time of a banking security framework, as all the facets of banking security come to play.

It was mentioned earlier that the RFI has posed some questions in which X9 has a security framework that can be applied to the critical infrastructure security. X9 standards are not a complete security solution or a framework by themselves, but may be considered the toolkit or building blocks that address selected security needs within the context of the whole framework. A percentage of the X9 encryption standards have now been identified in NIST standards, and a mutual agreement exists between X9 and NIST to address duplication. However, some banking/financial security needs go beyond other industry requirements, and may be unique in an implementation.

Security implementation within the banking and financial community is a collection of standards from various sources, including: X9, ISO, as ITU, IEEE, NIST and others. The emphasis within the financial community has and continues to be a transaction based or services based security standards. Costs and other factors continually reinforce the commitment to a standards approach.
Finally, we have provided a concise explanation of the X9 standards landscape so that NIST can gain an appreciation of how X9 security standards are available to markets beyond banking. Of course, this listing merely identifies what is currently available; there are always new standards

in queue. As NIST uses the results of the RFI to begin to build its anticipated "Cyberscurity Framework," it always has the option to contribute new item requests and to continue to participate as an active member of X9.

The X9 organization and community, with over 30 years of electronic banking and data security standards experience , has the background and expertise to provide a unique perspective and value in any initiative that looks to enhance and strengthen the payments and clearance infrastructure in the U.S. and global markets. X9 stands ready to be an ongoing resource to NIST (as well as to DHS, NSA, and OMB), as the federal government moves forward to build a meaningful Cybersecurity Framework and to advocate for implementation of strong security for critical infrastructure. As a public, consensus-based standards organization, X9 feels very strongly that such standards provide the best mechanism for success, rather than looking to an amalgam of private, proprietary standards that do not have the benefit of any public input. As NIST is well aware, OMB Circular A-119, which is predicated on the language and requirements of the National Technology Transfer Act of 1995, generally requires all federal agencies to use public consensus standards whenever possible, unless they can demonstrate to OMB why such standards are not appropriate. Accordingly, X9 offers its existing suite of security standards – as well as its expertise and the opportunity of future standards development – to NIST. We are willing to convene a panel of X9 security experts to meet with NIST to discuss what next steps would appropriate and useful.

X9 appreciates this opportunity to submit information to NIST in response to the RFI. If you have any questions or would like to follow up on our proposed next steps, please feel free to contact me.

Sincerely,

Cindy Fuller
X9 Executive Director

cc: Roy DeCicco, JP MorganChase – Chairman of X9 Board of Directors
Ed Scheidt, TecSec, Inc. – Board member, Chairman of X9 Subcommittee Data Security
X9 Board of Directors