FOR IMMEDIATE RELEASE

For further information:
Judith Vanderkay
jvanderkay@gmail.com
+1 (781) 883-3793

ASC X9 Publishes White Paper and Technical Report on Quantum Computing Risks; New Quantum Standard Effort Announced

ANNAPOLIS, Md. – March 12, 2019 **--** The Accredited Standards Committee X9 Inc. (X9) today announced the release of two documents on quantum computing: a white paper that seeks to educate the financial services industry about the risks that a large quantum computer would pose to the industry, and a Technical Report that describes both cryptographic and non-cryptographic uses for quantum computers, with associated issues. X9 also announced the launch of a new work group to develop a standard on quantum-safe solutions.

After 60 years of research and development, small working quantum computers now exist. It is predicted that large-scale stable quantum computers will be able to, in minutes, solve the intractable problems that the classes of cryptography protecting information on the Internet and in industry are based upon. These problems were originally selected because they are believed to be infeasible to solve on classical computing architectures, possibly requiring hundreds of thousands of years to compute, and thus providing a high degree of security. If quantum computers can reduce the solution times to minutes, they pose a major threat to these forms of cryptography.

White Paper X9.IR01-2019 -- "Quantum Computing Risks to the Financial Services Industry"
Created by the ASC X9 Quantum Computing Risk Study Group after more than a year of research, the paper provides background on the principles of quantum computing, and covers the state of the industry, quantum's threat to current cryptography, predictions about when this major threat may be realized, and actions that can be taken now to mitigate the risks. This paper will be updated as changes occur in the industry, and it is available for download at no charge.

Technical Report X9.TR-50 -- "Quantum Techniques in Cryptographic Message Syntax (CMS)"
This report discusses the basics of quantum computers and the quantum algorithms that break classical cryptography, and then shows how those algorithms could be used to attack classical cryptosystems, including secure authentication and communication. The report offers general recommendations for mitigating the impacts of quantum computing. It also provides a

background in the main branches of mathematics that are thought to yield quantum-safe cryptographic schemes. The report is also available for download at no charge.

New Quantum Computing Standard
As described in the new white paper and Technical Report, the advent of quantum computing will make cybersecurity attacks more difficult to prevent, placing the financial services industry at greater risk. Currently deployed standards may not offer sufficient security. The new standard will augment the extensible and algorithm-agnostic CMS messages in the current X9.73 standard, in order to help the financial services industry transition to quantum-safe solutions. The work has been assigned to X9's F4 subcommittee on Cybersecurity and Cryptographic Solutions. Interested parties are invited to participate in this effort.

"X9 has been out in front of the industry in recognizing the quantum threat and has begun the groundwork necessary to fortify our standards against quantum-enabled attackers," said Philip Lafrance, Standards Manager at ISARA Corporation, editor of the Technical Report and a participant in the creation of the white paper. "It has been a pleasure to work with such a qualified and experienced group of individuals in producing these two reports, and our collective mission is to continue to educate the community about the coming quantum threat, and successfully update our standards in time to mitigate it."

About the Accredited Standards Committee X9 Inc.
The Accredited Standards Committee X9 Inc. is a non-profit organization accredited by the American National Standards Institute (ANSI) to develop both national and international standards for the financial services industry. X9 has over 100 member companies and over 400 company representatives that work to develop and maintain approximately 100 domestic standards and 58 international standards.

The subjects of X9's standards include: retail and mobile payments; printing and processing of checks; corporate treasury functions; block chain technology; processing of legal orders issued to financial institutions; tracking of financial transactions and instruments; tokenization of data at rest; quantum computing risk; data breach; electronic contracts; and remittance data in business payments. X9 also performs the secretariat function, acts as the U.S. Technical Advisory Group, and provides the committee chair for ISO TC68, which produces international standards for the global financial services industry. For more information about X9 and its work, visit www.x9.org.

Follow ASC X9 on Facebook, LinkedIn and Twitter

###