September 9, 2016

Ms. Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 1070,
Gaithersburg, MD 20899

Re: Notice Seeking Public Comment on Current and Future States of Cybersecurity in the Digital Economy, Docket Number: 160725650-6650-01

Dear Ms. Grayson,

Credit Suisse ("CS") appreciates the opportunity to provide the National Institute of Standards and Technology ("NIST") with a response to the notice seeking public comment on the current and future states of cybersecurity in the digital economy.[1] In our response to NIST's request for input, we have focused our comments on future iterations of the NIST Framework for Improving Critical Infrastructure Cybersecurity ("Framework"), developing a cybersecurity lexicon, improving information sharing, refining processes and procedures for incident response, encouraging cybersecurity innovation and workforce development, understanding cybersecurity insurance, and increasing coordination between and among industry and regulators.

The constant integration of rapidly evolving technology into critical infrastructure makes it imperative we focus on continually enhancing cybersecurity, both internally and externally, and increase our coordination with our public- and private-sector partners. We find the below recommendations will contribute to keeping pace with the changing digital economy in the financial services sector.

I. NIST Framework

CS endorses the use of the Framework as a prominent method for owners and operators of critical infrastructure to improve cybersecurity risk management. We would like to join our sector-based coordinating council and associations, companies, and other entities in recognizing the success of the Framework, and the notable attention it has received since its launch in February 2014. The Framework is a cost-effective tool that recommends various standards, guidance, and best practices, and CS believes its success hinges on the avoidance of prescriptive solutions.

As such, CS supports the use of the Framework as a voluntary tool and suggests that financial services regulatory bodies align requests and examinations with the Framework. We also recommend the development of specific Framework extensions for each sector, maintaining a non-prescriptive approach, and keeping the overall Framework broad but tailoring its use or narrowing the scope to specific industries thus increasing its effectiveness. CS also encourages

[1] See NIST request for information (RFI) on the "Current and Future States of Cybersecurity in the Digital Economy." Docket Number 160725650-6650-01. Published on August 11, 2016.

NIST and the Department of Homeland Security's (DHS) C3 Voluntary Program to share lessons learned, and Framework usage best practices.

The use of the Framework is continuing to gain traction across all sectors and continues to be aligned to international standards and best practices. As Framework adopters, we recommend that NIST maintain its current role of fostering continued use of the Framework and providing incremental revisions to the Framework on a biennial cycle (every 2 years). It is our understanding that NIST will release a slightly revised version of the Framework in 2017, and CS is hopeful that NIST will continue to seek industry feedback on future iterations of the Framework. Among other areas, CS sees a need for the Framework to address supply chain risk management and privacy standards. Although many organizations have robust internal risk management processes, supply chain criticality and dependency analysis, collaboration, information sharing, and trust mechanisms remain a challenge. The Framework should promote the mapping of existing supply chain risk management standards, practices and guidelines to the Framework Core.

As an international bank, we are particularly pleased that the Framework was designed with international adoption in mind. We encourage NIST to maintain this approach in the future. CS reiterates its support of the Framework and encourages the next administration to continue to promote its use.

II. Cybersecurity Lexicon

Cybersecurity is ever-changing, and many cyber terms continue to emerge. CS recognizes previous efforts by the U.S. Government, both by NIST and other joint public sector organizations, to develop and maintain a Cybersecurity Glossary. We recognize the highly intensive effort it takes to maintain reference documents and appreciate these efforts. We acknowledge that an effective glossary must be in a continuous state of coordination and improvement.

CS sees an opportunity for the development and maintenance of a mutually beneficial "Cybersecurity Glossary" that will save industry and regulators time and resources during examinations. The Cybersecurity Glossary should reference commonly used terms and concepts in regulatory examinations and align with commonly used terms in the Framework and other NIST publications. Additionally, we encourage regulators to refer to this new glossary or an alternative existing cybersecurity reference document for regulatory reporting efforts. We also see a cybersecurity lexicon as useful tool for industry when considering the scope of cyber insurance, a still somewhat new entrant to the marketplace, which, if executed correctly, has the potential to promote good cyber hygiene.

III. Information Sharing

The Cybersecurity Information Sharing Act (CISA) seeks to incentivize industry and the U.S. Government to exchange data on cybersecurity threats and vulnerabilities. CS recognizes that as additional information sharing efforts are undertaken, the United States will be better prepared to take on a wide variety of cybersecurity threats and vulnerabilities. In the spirit of CISA, CS recommends expanding public-private information sharing initiatives to include more intensive and rapid information sharing, more sophisticated analysis, and deeper collaboration among large financial services firms and government agencies. Additionally, we are hopeful that

the information sharing dialogue can expand beyond bi-directional sharing and include more international approaches to information sharing.

CS endorses the use of existing forums and channels for information sharing, but we highlight our concern that banks are providing more information to the government than we are receiving. We reassure the government that sharing actionable information at an increased rate will result in a mutually beneficial outcome. Additionally, CS recommends development of an annual inventory of cybersecurity information sharing forums and products that are available to the private sector. As we are encouraged information sharing will continue to improve, CS reiterates the importance of limited liability protection for those entities that voluntarily share information and report incidents.

As a foreign banking organization (FBO), CS implemented Section 165 of the Dodd-Frank Act, namely enhancing prudential standards covering risk governance, risk-based capital and leverage requirements, as well as liquidity management and capital planning. As an FBO the Federal Reserve rule required CS's U.S. subsidiaries to be placed underneath a top-tier U.S. intermediate holding company (IHC). As such, we recently submitted our membership to the Financial Services Sector Coordinating Council so we can contribute to joint information sharing efforts within the financial services sector.

As a current member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), CS recognizes the benefit of receiving physical and cyber threat alerts and other critical information. Additional guidance around applying the outputs of automated indicators from cyber threat intelligence feeds is needed based on current threat standardization models (i.e., STIX, TAXII, and CybOX). CS encourages expanding indicator sharing initiatives to include tools and best practices for indicator management.

CS is encouraged by movements toward solidifying stronger public-private partnerships and looks forward to future collaboration across other industry sectors and with regulatory bodies in addressing cyber risks.

IV. Incident Response

As an extension of efforts undertaken to improved information sharing, CS believes there is a need to improve processes and procedures for defining, reporting, and responding to sector incidents and a need to promote a more effective cyber exercise and simulations program. We recommend clarifying roles and responsibilities for incident response, including how information related to specific incidents will be handled.

CS encourages the U.S. Government to engage private sector organizations prior to, during, and following sector incidents. Additionally, we suggest defining requirements for reporting of cyber incidents and work to introduce more specificity into what information needs to be reported and to whom. CS is also interested in helping to shape the role international organizations can contribute to incident response. Additionally, CS recommends working with potential partners to promote a clear, concise framework for reporting data breaches. Specific data breach notification requirements are needed to provide clarity on reporting for banks.

Private sector dependency on critical infrastructure requires that business continuity plans be updated and tested regularly. In general, there is a growing need to be trained on how to prepare and react to small and large scale cyberattacks against critical infrastructure. Disruptions

to our current lifestyle (e.g., short term consumption, e-commerce, e-money, and digital information exchange) could produce cascading effects and result in catastrophic damage.

V. Cybersecurity Education, Workforce Development, and Innovation

The National Initiative for Cybersecurity Education (NICE) promotes a robust dialogue around cybersecurity education and workforce development. New and evolving cybersecurity requirements for employees require organizations to promote a culture of secure and ethical usage of Internet connected devices and software. CS encourages government and private-sector partnerships, in coordination with academia, to continue to build on existing successful programs like NICE to increase the number of skilled cybersecurity professionals. CS also believes workforce development is a major issue, and one that should be addressed in the Framework. The Framework should include additional guidance for cybersecurity education across all levels of an organization. Additionally, CS encourages DHS and other government organizations to continue cybersecurity awareness activities, including the National Cyber Security Awareness Month (NCSAM) initiative designed to engage and educate public- and private-sector partners.

Additionally, CS is committed to maintaining mentorship opportunities with incubator and technology accelerator programs. We encourage government support of similar initiatives to improve technology, services, and/or software vendors, including efforts such as "bug bounty hunting" and "hacking camps" to improve the cybersecurity posture of existing critical infrastructure. CS has embarked on a mission to foster a culture of innovation and deliver the capabilities and resources needed to support transformational concepts with the potential to transform the entire financial sector. Innovation has been identified as a core competency for the world's most successful companies. CS recommends the government encourage a culture of innovation to address changing technologies and security concerns.

VI. Cybersecurity Insurance

While cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, there is a need to better understand the value of protected assets and the scope of insurance coverage. While the cyber insurance industry is still expanding, CS sees an opportunity for regulators and organizations like NIST to engage critical infrastructure cybersecurity stakeholders, including the insurance industry, when developing and demonstrating the utility and effectiveness of standards, procedures, and other measures. Cybersecurity insurance carriers would bring extensive knowledge of the effectiveness of specific cybersecurity practices and could help evaluate specific proposed elements from their unique perspective. This collaboration could serve as a basis for creating underwriting practices that promote the adoption of cyber risk-reducing measures and risk-based pricing. This could also foster a competitive cybersecurity insurance market

VII. Coordination amongst industry, between regulators and industry, and amongst regulators

CS supports robust coordination amongst industry, between regulators and industry, and amongst regulators to ensure a mutually beneficial approach to safeguarding information technology and computer systems. We strongly encourage regulators to work with the financial services industry to develop a viable approach to address regulators' need to evaluate security, while satisfying institutions' need to minimize risk. We also see a need to harmonize the different

approaches that State, Federal, and International regulators take with the financial services industry to better coordinate our efforts. We echo our previous support for financial services regulatory bodies at all levels of government to align their requests with the Framework.

As technology continues to evolve, we recognize that future regulation will need to be principals based and adaptive to the ever changing needs of safely operating in a digital economy, and we encourage best practices to combat cyber threats. The financial services industry is already addressing security concerns around future regulatory topics, including cloud computing, penetration testing and operational assessments, third party risk management, and the Internet of Things. As an international organization, CS is actively working to make continual improvements to protecting customers' data and our infrastructure both internally and with the guidance of both domestic and international regulators. We look forward to bringing our expertise to the table with regulatory authorities around the globe to work towards harmonizing emerging requirements and minimizing cyber risks.

CS finds that the all parties benefit when the private sector can shape, in close collaboration with public-sector stakeholders, the development and revision of cybersecurity safeguards that industries implement.

***

We thank NIST for the opportunity to provide our input. If you have any questions, please do not hesitate to contact the undersigned or Joseph Seidel at 202-626-3302.

Roben Dunkin
Head of Technology
Credit Suisse Holdings USA
One Madison Avenue, NY, NY 10010
Phone +1 212-325-0976

Alicja Cade
Chief Information Security Officer
Credit Suisse Holdings USA
One Madison Avenue, NY, NY 10010
Phone +1 212-325-4416