MEMORANDUM OF UNDERSTANDING

Between

DEPARTMENT OF HOMELAND SECURITY
Science and Technology Directorate

And

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

And

FINANCIAL SERVICES SECTOR COORDINATING COUNCIL
for Critical Infrastructure Protection and Homeland Security

This Memorandum of Understanding (MOU) is by and among the National Institute of Standards and Technology (NIST) an agency of the Department of Commerce, the Science and Technology Directorate (S&T) of the Department of Homeland Security (DHS), and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) (taken together "Parties"). The Parties agree that it is in the best interests of the Parties and the American people to develop a strategic partnership for cybersecurity. The Parties will endeavor to leverage their core cybersecurity expertise, research and development capabilities, and resources under separate Project instruments (1) to facilitate innovation, (2) to identify and overcome cybersecurity vulnerabilities, and (3) to develop more efficient and effective cybersecurity processes that benefit critical financial services functions and may also benefit other critical infrastructures.

1. PURPOSE.

This MOU formalizes the intent of the Parties to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes based upon the financial services sector's needs. The activities will leverage the expertise of each of the Parties to develop and test innovative cybersecurity technologies and processes aimed at strengthening the resiliency, security, integrity, and usability of financial services sector critical infrastructures.

2. BACKGROUND.

DHS leads the United States Government's unified national efforts to secure and protect the country. S&T is DHS's primary research and development arm. S&T works to improve homeland security by providing to the Department, and state, local, tribal, and territorial emergency responders and officials state-of-the-art technologies and processes that help them achieve their missions. An important mission of S&T is to conduct research and develop advanced cybersecurity and information assurance technologies and processes to secure the Nation's current and future cyber and critical infrastructures. S&T conducts a substantial portion of its research in cooperation with other Federal agencies, state, local, and tribal governments, universities, and private industry.

NIST develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST's mission is carried out intramurally through scientific research in six major laboratories, as well as extramurally, in close collaboration with U.S. industry, academia, and international organizations.

The FSSCC supports research and development initiatives to protect the physical and electronic infrastructure of the Banking and Finance Sector and to protect its customers by enhancing the Sector's resiliency and integrity. The FSSCC established the Research and Development Committee in 2004 as a standing committee to identify priorities for research, promote development initiatives to significantly improve the resiliency of the Financial Services Sector, engage stakeholders (including academic institutions and government agencies), and coordinate these activities on behalf of the Banking and Finance Sector.

This MOU provides a framework under which two or more of the Parties may join in separate instruments to accomplish specific Projects that combine the complementary roles of the Parties. Such Projects will be directed toward the development and delivery of innovative cybersecurity technologies and processes supporting the critical role of financial services in homeland security. In addition, the Parties will coordinate with the Department of Treasury, as appropriate, in its role as the financial services sector-specific agency under Homeland Security Presidential Directive (HSPD) 7.

3. AUTHORITIES.

The National Institute of Standards and Technology enters into this MOU pursuant to 15 U.S.C. § 272(b)(10), (b)(11), (c)(12) and (c)(14). The Science and Technology Directorate of the Department of Homeland Security enters into this MOU pursuant to section 302 of the Homeland Security Act of 2002 (6 U.S.C. § 182). Both agencies are participating pursuant to HSPD 7, which establishes a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them.

4. AGREEMENT.

The Parties intend to work together under separate instruments between two or more of the Parties to facilitate the development and implementation of new innovative cybersecurity technologies, processes, and practices (Projects). These Projects may include but are not limited to:

A. COOPERATION AND COORDINATION

- Coordinating the design, development, and delivery of innovative cybersecurity technologies and processes.

B. INFORMATION SHARING

- Sharing ideas and concepts for better cybersecurity, including improved effectiveness and enhanced efficiency.

C. DEVELOPMENT AND IMPLEMENTATION OF JOINT TEST INFRASTRUCTURES

- Engaging in cooperative planning and development of joint test infrastructure activities.
- Developing use cases and the supporting test plans to explore the facilitation of high assurance network infrastructures, advanced identity management technologies, and improved usability of security technologies.

5. PERIOD OF AGREEMENT.

a. This MOU will take effect when signed and dated by the last of the signing Party and will be effective for five years. The Parties may extend this MOU in writing by mutual agreement of the Parties.

b. The Parties shall review this MOU annually. As a result of that review or otherwise, the Parties may alter this MOU by written amendment signed by the signing officials or their successors.

6. PROJECTS.

This MOU does not detail how collaborative research efforts will be implemented and administered. The Parties may enter into separate instruments for Projects to be undertaken pursuant to this MOU. Such instruments may address the particular scope of work; the

Parties' roles and responsibilities in the Project; the administration, coordination and implementation of the Project; relevant background information; the respective rights of each Party to own, use, and license intellectual property that may be created in the course of the Project; any confidentially provisions; and other appropriate issues.

7. NO FUNDING.

This MOU creates no obligation on any of the Parties and provides no funds to any of the Parties. Pursuant to Paragraph 6 above, Projects undertaken pursuant to this MOU shall be separately negotiated and be the subject of a separate instrument. Each Party to this MOU is responsible for its own costs, unless otherwise provided for in a subsequent, written Project instrument.

8. DISPUTE RESOLUTION.

Any disagreement of one or more of the Parties that cannot be resolved at the working levels shall be submitted to the signers or their successors for final resolution.

9. TERMINATION.

Any Party may terminate its participation in this MOU with 30 days advanced written notice to the other Parties. Termination of this MOU will not affect the obligations of the terminating or remaining Party(ies) in the performance of any Project instruments that may be in place at the time of the effective date of the Termination.

APPROVAL/SIGNATURES

S&T/DHS — Date: 12/2/10

NIST/DoC — Date: DEC 0 2 2010

FSSCC — Date: 12/6/10