MEMORANDUM OF AGREEMENT BETWEEN

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

AND

THE NATIONAL PROTECTION AND PROGRAMS DIRECTORATE (NPPD)

REGARDING CYBERSECURITY

1. PARTIES. The parties to this Agreement are the National Institute of Standards and Technology (NIST), U.S. Department of Commerce (DOC) and the National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security (DHS).

2. AUTHORITY. This Agreement is authorized under the provisions of chapter 35 of title 44, United States Code ("Coordination of Federal Information Policy"), including the Federal Information Security Management Act of 2002 (44 USC § 3541 et seq.); the Homeland Security Act (2002), 6 U.S.C. § 101 et seq.; 15 U.S.C. §§ 272(b)(1)(3)(11), (c)(13)(14) and 15 USC §§ 278g-3 and 278g-4 ("National Institute of Standards and Technology"); Office of Management and Budget (OMB) Circular A-130; OMB Circular A-119; OMB Memorandum M-10-28; Homeland Security Presidential Directive 7 ("Critical Infrastructure Identification, Prioritization, and Protection"); and National Security Presidential Directive 54/Homeland Security Presidential Directive 23 ("Cybersecurity Policy").

3. PURPOSE. The purpose of the Agreement is to set forth terms by which NIST and NPPD will collaborate in the performance of their cybersecurity responsibilities, increase communication between their cybersecurity personnel, and improve coordination of interrelated activities.

4. SCOPE. NIST and NPPD agree to collaborate to improve the synchronization and mutual support of their respective efforts to improve the nation's cybersecurity while protecting privacy and civil liberties. This Agreement is intended to improve the cybersecurity programs of both parties by establishing mutually beneficial activities and exchanges. It does not alter existing DOC or DHS authorities or oversight relationships, nor is it intended to replicate or aggregate the diverse line organizations that collectively execute cybersecurity missions across technology and standards development, operations, or customer support functions.

5. RESPONSIBILITIES.

    a. National Institute of Standards and Technology will:

i. Identify and assign, in coordination with NPPD, an appropriate NIST official to coordinate cybersecurity activities with NPPD. This cybersecurity coordinator will be detailed to an NPPD facility.

ii. Consult with NPPD on information security standards, guidelines, and frameworks developed by NIST to ensure that federal Departments and Agencies and critical infrastructure can implement standards, guidelines, and frameworks at a practical operational level, based on risk.

iii. Notify NPPD in advance when NIST intends to provide an opportunity for public comment on proposed standards, guidelines, or frameworks.

iv. Provide technical expertise to NPPD regarding the application of NIST-developed standards, guidelines, and frameworks; detection and handling of information security incidents; development of cybersecurity vulnerability assessments; and security automation.

v. Enable NPPD participation in NIST-led engagements with industry focused on enhancing public and private sector cooperative partnerships or improving cybersecurity and participate in similar DHS-led engagements, including boards and advisory groups, when appropriate.

vi. In accordance with 15 U.S.C. 278g-4(a)(3), appoint one representative from DHS to the Information Security and Privacy Advisory Board (ISPAB).

b. National Protection and Programs Directorate will:

i. Identify and assign, in coordination with NIST, an appropriate NPPD official to coordinate cybersecurity activities with NIST. This cybersecurity coordinator will be detailed to a NIST facility.

ii. Consult with NIST on the production of bulletins or memoranda pertaining to implementation of standards, guidelines, frameworks or other applicable cybersecurity policies.

iii. Consult with NIST on the development of metrics that will be used by Departments and Agencies to measure the effectiveness of cybersecurity programs or to identify optimal security solutions.

iv. Coordinate with NIST personnel to develop or enhance existing cybersecurity vulnerability assessments for Departments and Agencies and critical infrastructure

v. Provide relevant information, including analyses, priorities, sector specific plans, vulnerability assessments, and reports on operational aspects of Federal agency cybersecurity, consistent with NPPD information sharing policies, to assist NIST in the development of information security standards, guidelines, and frameworks.

c. NIST and NPPD will jointly:

i. Establish Technical Working Groups, as necessary, to review and analyze issues of mutual interest and recommend courses of action for maximizing efficiencies, avoiding duplication of efforts, ensuring appropriate consistency in products produced by either party, and providing cost effective cyber security solutions for Federal agencies, critical infrastructure, and industry.

ii. Improve coordination between NPPD and NIST, to facilitate the identification and sharing of relevant information and to ensure effective utilization of such information.

iii. Coordinate the development of cybersecurity guidance and recommendations to ensure that information provided by both NIST and NPPD is as practical, timely, complete, and cost-effective as possible.

iv. Engage federal, state, tribal, territorial, and local entities, as well as private sector communities, to obtain input on cybersecurity guidance and recommendations by involving a broad range of appropriate stakeholders.

v. Encourage the use of employee detail assignments between NIST and NPPD to ensure that technical and policy matter expertise is shared between agencies and to support staff training in operational and research areas.

6. OVERSIGHT. To oversee the activities described in the preceding paragraphs, the Director of NIST or the Director of the NIST Information Technology Laboratory and the NPPD Deputy Under Secretary for Cybersecurity or the Assistant Secretary for Cybersecurity and Communications, or their designees, will meet quarterly to review the activities in this Agreement.

7. POINTS OF CONTACT.

   a. The NIST point of contact for this Agreement is Charles H. Romine, Director of the Information Technology Lab.

   b. The DHS point of contact for this Agreement is Mark Weatherford, NPPD Deputy Undersecretary for Cybersecurity.

8. OTHER PROVISIONS. Nothing in this Agreement is intended to conflict with law, regulation, Presidential order or directive, or the directives of DOC or DHS. If a term of this Agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this Agreement shall remain in full force and effect. This Agreement shall be interpreted and implemented in a manner that respects, complies with, and does not abrogate the statutory and regulatory responsibilities of the Secretary of Commerce and Secretary of Homeland Security. This Agreement does not obligate funds or create a financial obligation between the parties. All activities contemplated by this Agreement are subject to the availability of funds and other necessary resources to the parties.

9. EFFECTIVE DATE. This Agreement is effective upon signature of both parties.

10. MODIFICATION AND REVIEW. This Agreement may be modified upon the mutual written consent of the parties. This Agreement will be reviewed by the parties after one year.

11. TERMINATION. The terms of this Agreement, will remain in effect for a period of five (5) years from the Effective Date. This Agreement may be extended for additional five (5) year periods by written amendment executed by both parties. Either party, upon 30 days written notice to the other party, may terminate this Agreement.

APPROVED BY:

PATRICK GALLAGHER
Under Secretary
Standards and Technology
Department of Commerce

DATE: 12 Feb 2013

RAND BEERS
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

DATE: 2/11/13