MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
AND
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY (NSA)
CONCERNING
THE IMPLEMENTATION OF THE
FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002

Recognizing that:

A: The Federal Information Systems Management Act of 2002 (Title III of Public Law 107-347) superseded the Computer Security Act of 1987 (PL 100-235) and preserved earlier authorities of NIST to develop information security standards and guidelines for information security, including systems operated by a contractor for an agency, but such standards and guidelines do not apply to national security systems. The Act requires NIST to consult with other agencies and offices (including the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security), and with the private sector to improve information security and avoid unnecessary and costly duplication of effort; and to ensure that standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems.

B: Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Information Security and Privacy Advisory Board (ISPAB), at least one of whom shall be from the NSA.

C: The National Security Agency (NSA), pursuant to National Security Directive 42, establishes standards for national security systems and, may upon request, provide technical assistance for the protection of national security systems as defined in 44 U.S.C. § 3542(b)(2).

D: NSA, pursuant to section 2.6(c) of Executive Order (E.O.) 12333, as amended, may provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency. When lives are in danger, NSA may provide this support to local law enforcement agencies. Provision of expert personnel authorized under section 2.6(c) of E.O. 12333 must be approved by the General Counsel of the providing entity. Pursuant to section 2.6(d) of E.O. 12333, as amended, NSA also may provide technical assistance to civil authorities.

E: NIST, pursuant to 15 U.S.C. § 278g-3, develops standards, guidelines, and associated methods and techniques for non-national security information systems and provides technical assistance to agencies, upon request, regarding compliance with the standards and guidelines, detecting and handling information security incidents, and information security policies, procedures, and practices. In addition, pursuant to 15 U.S.C. § 273, NIST is authorized to exercise its functions for the Government of the United States and for international organizations of which the United States is a member; for governments of friendly countries; for any State or municipal government within the United States; or for any scientific society, educational institution, firm, corporation, or individual within the United

States or friendly countries engaged in manufacturing or other pursuits requiring the use of standards or standard measuring instruments: Provided, That the exercise of these functions for international organizations, governments of friendly countries and scientific societies, educational institutions, firms, corporations, or individuals therein shall be in coordination with other agencies of the United States Government, in particular the Department of State in respect to foreign entities.

F. In 1989, the Directors of NIST and NSA approved a Memorandum of Understanding on the implementation of PL 100-235, formalizing cooperation between the NIST and the NSA, and instituting a Technical Working Group (TWG) to review and analyze issues of mutual interest pertinent to the protection of systems that process sensitive or other unclassified information. The work of the TWG has contributed to the adoption of a set of public NIST Federal Information Processing Standards and Special Publications for cryptographic algorithms that is internationally accepted and used to protect ordinary e-commerce, non-national security information, and national security information.

Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

I. The NIST shall:

1. In accordance with 15 U.S.C. 278g-4(a)(3), appoint to the ISPAB at least one representative from the NSA.

2. Draw upon information security and cyber security technical guidelines and standards developed by the NSA for national security systems to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting Federal non-national security systems and the information that resides therein.

3. Consult with NSA, as appropriate, to conduct or initiate research and develop information security, cyber security, and cryptographic associated methods and techniques that include, but are not limited to, trusted technology, security automation techniques, and personal identification methods.

4. Develop information security and cyber security standards, guidelines, and associated methods and techniques for protecting non-national security systems and the information that resides therein, drawing upon the expertise, products, services and commercial partnership activities of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.

5. Avoid duplication of NIST and NSA effort, where possible, by entering into mutually agreeable arrangements.

6. Consult with NSA on all matters related to cryptographic algorithms and cryptographic techniques for non-national security applications, including, but not limited to research, development, evaluation, or their inclusion into standards prior to the public release of information concerning these matters and request NSA's assistance as needed.

7. As appropriate, utilize NSA's technical resources to provide technical assistance to NIST's customers as specified above in paragraph E.

II. The NSA shall:

1. Nominate one representative to the ISPAB, identified by the Director of NSA.

2. Draw upon information security and cyber security technical guidelines and standards developed by the NIST for non-national security systems to the extent that the NSA determines that such guidelines are consistent with the requirements for protecting national security systems and the information that resides therein.

3. Provide the NIST with technical guidelines in trusted technology, information security, cyber security, and personal identification that may be used in cost-effective systems for protecting non-national security systems.

4. Consult with NIST, as appropriate, to conduct or initiate research and develop information security, cyber security, and cryptographic associated methods and techniques that include, but are not limited to, trusted technology, security automation techniques, and personal identification methods.

5. Be responsive to NIST requests for assistance including, but not limited to, all matters related to cryptographic algorithms and cryptographic techniques, information security, and cybersecurity.

6. Upon request by Federal agencies, their contractors, and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend solutions to secure systems against that threat.

III. The NIST and the NSA shall:

1. Exchange technical standards and guidelines, as necessary, to achieve the purposes of the Act.

2. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

3. Maintain a dialogue to ensure that each organization remains abreast of emerging technologies and issues affecting information security and cyber security.

4. Continue the Technical Working Group established under the 1989 MOU to review and analyze issues of mutual interest pertinent to the protection of non-national security systems. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Director for Information Assurance or the NIST Information Technology Laboratory (ITL) Director, or may be generated and addressed by the group.

5. Ensure the Technical Working Group reviews, prior to public disclosure, all matters regarding technical systems security techniques to be developed for use in protecting non-national security

systems and the information that resides therein, to ensure they are consistent with the national security of the United States.

6. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

7. On an annual basis, or as otherwise mutually agreed to by NIST and NSA, the NSA Director for Information Assurance and the NIST Director of the Information Technology Laboratory or their designees will review the work that was performed under this MOU.

8. Activities conducted pursuant to this MOU are subject to the availability of funds and other necessary resources to the parties. No funds are obligated by this MOU.

IV. Points of Contact: The NIST point of contact for this MOU is the Director of the Information Technology Laboratory (301) 975-2900. The NSA point of contact is the Director of Information Assurance (301) 688-8111.

V. Either party may elect to terminate this MOU upon six months written notice.

This MOU is effective upon approval of both signatories.

PATRICK GALLAGHER
Director
National Institute of Standards and Technology
DATE: 23 - Dec - 2010

KEITH B. ALEXANDER
General, U. S. Army
Director, National Security Agency
DATE: 19 Aug 10