MEMORANDUM OF AGREEMENT

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY

AND

THE DEPARTMENT OF DEFENSE

REGARDING CYBERSECURITY

1. PARTIES. The parties to this Agreement are the Department of Homeland Security (DHS) and the Department of Defense (DoD).

2. AUTHORITY. This Agreement is authorized under the provisions of the Homeland Security Act (2002); the Economy Act; U.S. Code Title 10; Executive Order 12333; National Security Directive 42; Homeland Security Presidential Directive-5; Homeland Security Presidential Directive-7; and National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

3. PURPOSE. The purpose of the Agreement is to set forth terms by which DHS and DoD will provide personnel, equipment, and facilities in order to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities. Implementing this Agreement will focus national cybersecurity efforts, increasing the overall capacity and capability of both DHS's homeland security and DoD's national security missions, while providing integral protection for privacy, civil rights, and civil liberties.

4. SCOPE. DoD and DHS agree to collaborate to improve the synchronization and mutual support of their respective efforts in support of U.S. cybersecurity. Departmental relationships identified in this Agreement are intended to improve the efficiency and effectiveness of requirements formulation, and requests for products, services, technical assistance, coordination, and performance assessment for cybersecurity missions executed across a variety of DoD and DHS elements. They do not alter existing DoD and DHS authorities, command relationships, or privacy, civil liberties, and other oversight relationships. In establishing a framework to provide mutually beneficial logistical and operational support, this Agreement is not intended to replicate or aggregate unnecessarily the diverse line organizations across technology development, operations, and customer support that collectively execute cybersecurity missions.

5. RESPONSIBILITIES.
   A. Department of Homeland Security.
      1) Identify and assign, in coordination with the Department of Defense, a DHS Director, Cybersecurity Coordination who will be in the National Protection and

CLEARED
For Open Publication

OCT 13 2010

Office of Security Review
Department of Defense

10

11-S-0123

Programs Directorate and will be located at the National Security Agency (NSA) but will not be in the NSA chain of command. This individual will also act as the DHS Senior Cybersecurity Representative to U.S. Cyber Command (USCYBERCOM).

2) Receive DoD requests for cybersecurity support and consider DoD requirements, as appropriate and consistent with applicable law and DHS mission requirements and authorities, related to operational planning and mission coordination.
3) Identify qualified DHS personnel to perform DHS functions under the sole supervision and direction of DHS officials as follows:
   a. Assign DHS personnel to work at NSA as part of a Joint Coordination Element (JCE) performing the functions of joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity under the direct supervision of the Director, Cybersecurity Coordination;
   b. Assign personnel to work at the NSA Directorate of Acquisition for collaborative acquisition and technology development;
   c. Assign or detail, as appropriate, personnel to work at the National Security Agency/Central Security Services (NSA/CSS) Threat Operations Center (NTOC) to promote joint operational planning, coordination, synchronization, requirement translation, and other DHS mission support for homeland security for cybersecurity; and
   d. Assign representatives from the Office of the General Counsel, Privacy Office, and the Office for Civil Rights and Civil Liberties to support the DHS Director, Cybersecurity Coordination, at NSA, and coordinate with the DoD counterparts identified in paragraph B.2.d.
4) Ensure that DHS personnel have current security clearances (TS/SCI) upon assignment to NSA, including training on the appropriate handling and dissemination of classified and sensitive information in accordance with DoD, Intelligence Community and NSA regulations.
5) Provide funding for DHS mission requirements, salaries, and training unique to DHS personnel for assignments under paragraph 5.A.3.
6) Provide appropriate access, administrative support, and space for an NSA Cryptologic Services Group (CSG) and a USCYBERCOM Cyber Support Element (CSE) collocated with the National Cybersecurity and Communications Integration Center (NCCIC), at DHS, and integration into DHS's cybersecurity operational activities. DHS will provide all necessary DHS equipment and connectivity to permit both CSG and CSE entities the capability to carry out their respective roles and responsibilities.
7) DHS Director, Cybersecurity Coordination.
   a. Provide requests for cybersecurity planning, technology, and where appropriate other support to NSA and USCYBERCOM and advocate for such requests based on DHS requirements to protect Federal Executive branch, non-DoD, non-national security systems, and U.S. critical infrastructure and key resources.
   b. Convey to and coordinate within DHS any NSA and USCYBERCOM requests for support or requirements regarding cybersecurity operations.

c. Participate in and lead, as appropriate, joint planning and other processes.
d. Promote and facilitate strong communications between DHS and DoD senior leadership, including that of NSA, on cybersecurity matters of joint interest, including engaging in joint operational planning and mission coordination.
e. Maintain cognizance of DHS and, as appropriate, of DoD, NSA, and USCYBERCOM cybersecurity activities, to assist in deconfliction and promote synchronization of those activities.
f. Assist in coordinating DoD and DHS efforts to improve cybersecurity threat information sharing between the public and private sectors to aid in preventing, detecting, mitigating, and/or recovering from the effects of an attack, interference, compromise, or incapacitation related to homeland security and national security activities in cyberspace.

B. Department of Defense.
1) Direct the Director of NSA (DIRNSA) and Commander, USCYBERCOM, to undertake collaborative activities and provide cybersecurity support envisioned in this agreement and subsequent implementing agreements.
2) National Security Agency.
a. Assign an NSA SES-equivalent to serve as the NSA lead to the Joint Coordination Element (JCE). This NSA official will coordinate and work with the DHS Director, Cybersecurity Coordination in carrying out the activities of the Joint Coordination Element. This NSA official will not be in the DHS chain of command, and his or her performance ratings will be prepared by NSA with input from the DHS Director, Cybersecurity Coordination. This NSA official will supervise and direct all NSA personnel assigned to the JCE.
b. Receive and coordinate DHS requests for cybersecurity support and consider DHS requirements, as appropriate and consistent with applicable law and NSA mission requirements and authorities, in operational planning and mission coordination.
c. Provide appropriate access, facilities, and administrative support (including necessary equipment and connectivity) to support the Director, Cybersecurity Coordination and DHS personnel assigned or detailed to the three entities listed below. NSA will provide all necessary NSA equipment and connectivity to permit DHS personnel with the capability to carry out their roles and responsibilities.
i. NSA Directorate of Acquisition
ii. Joint Coordination Element to be located at NSA
iii. NSA/CSS Threat Operations Center
d. Identify representatives from its Office of the General Counsel and Privacy Office to work with counterparts at DoD, USCYBERCOM, and DHS to support the implementation of this Agreement.
e. Collocate a Cryptologic Services Group at the NCCIC at DHS, for support to and operational synchronization with DHS's cybersecurity operations and the National Cyber Incident Response Plan (NCIRP).
f. Assign or detail qualified personnel in accordance with this Agreement both to serve in JCE positions and in CSG positions as mutually agreed.

g. Engage with DHS and USCYBERCOM in joint operational planning and mission coordination.
h. Provide funding for NSA mission requirements, salaries and training unique to NSA for personnel identified in B.2.c.

3) USCYBERCOM.
a. Receive DHS requests for cybersecurity support and consider DHS requirements, as appropriate and consistent with applicable law and USCYBERCOM mission requirements and authorities, in operational planning and mission coordination.
b. Collocate a Cyber Support Element at the NCCIC at DHS, for support to and operational synchronization with DHS's cybersecurity operations and the NCIRP.
c. Assign qualified personnel to CSE positions.
d. As needed to implement this Agreement, provide, on a reimbursable basis, appropriate access, administrative support and space for DHS personnel.
e. Provide funding for USCYBERCOM mission requirements and training unique to its personnel during the assignment.
f. Engage with DHS and NSA in joint operational planning and mission coordination.

C. Joint DoD-DHS.
1) Synchronize the roles and relationships of the proposed DoD Integrated Cyber Center (ICC) and the current DHS National Cybersecurity and Communications Integration Center (NCCIC).
2) Develop agenda of appropriate supporting actions, including consideration of the establishment of a Joint Program Office (JPO).
3) Develop jointly appropriate agreements, including necessary funding mechanisms, to implement the objectives and responsibilities of this Agreement pursuant to applicable authority.

6. OVERSIGHT. To oversee the activities described in the preceding paragraphs, the Deputy Secretary of Homeland Security and the Deputy Secretary of Defense will conduct monthly oversight meetings supported by the DHS Deputy Under Secretary, National Protection and Programs Directorate (NPPD); the Principal Deputy Under Secretary of Defense for Policy and the Director of NSA/Commander, USCYBERCOM.

7. POINTS OF CONTACT.

Philip Reitinger
Deputy Under Secretary
National Protection and
Programs Directorate
Department of Homeland Security
Washington, DC 20528
(703) 235[redacted]

James N. Miller
Principal Deputy Under Secretary
of Defense for Policy
Department of Defense
2100 Defense Pentagon
Washington, DC 20301-2100
(703) 697[redacted]

8. OTHER PROVISIONS. Nothing in this Agreement is intended to conflict with law, regulation, Presidential order or directive, or the directives of DHS or DoD. 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 and complies with (and does not abrogate) the statutory and regulatory responsibilities of the Secretary of Homeland Security and the Secretary of Defense. This Agreement does not obligate funds.

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, as modified with the consent of both parties, will remain in effect until terminated. Either party upon 30 days written notice to the other party may terminate this Agreement.

APPROVED BY:

Janet Napolitano

Secretary of Homeland Security

Date: 9-27-10

Robert Gates

Secretary of Defense

Date: 9-24-10