



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

AUG 09 2013

CHIEF INFORMATION OFFICER

MEMORANDUM FOR DEPARTMENT OF STATE, CHIEF INFORMATION OFFICER
DEPARTMENT OF THE TREASURY, CHIEF INFORMATION OFFICER
DEPARTMENT OF JUSTICE, CHIEF INFORMATION OFFICER
DIRECTOR OF NATIONAL INTELLIGENCE, CHIEF INFORMATION OFFICER
CENTRAL INTELLIGENCE AGENCY, CHIEF INFORMATION OFFICER
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, CHIEF INFORMATION OFFICER
NATIONAL SECURITY STAFF, CHIEF INFORMATION OFFICER
OFFICE OF NATIONAL DRUG CONTROL POLICY, CHIEF INFORMATION OFFICER
DEPARTMENT OF TRANSPORTATION/MARITIME ADMINISTRATION, CHIEF INFORMATION OFFICER
UNITED STATES GEOLOGICAL SURVEY, CHIEF INFORMATION OFFICER
FEDERAL AVIATION ADMINISTRATION, CHIEF INFORMATION OFFICER
NUCLEAR REGULATORY COMMISSION, CHIEF INFORMATION OFFICER
FEDERAL COMMUNICATIONS COMMISSION, CHIEF INFORMATION OFFICER
GOVERNMENT ACCOUNTABILITY OFFICE, CHIEF INFORMATION OFFICER

SUBJECT: Improving Security of Federal Department and Agency Connections to the Department of Defense Secret Internet Protocol Router Network

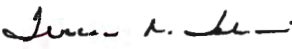
Cybersecurity reviews of several Federal Department and Agency connections to the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNET) highlight the need to strengthen security, more effectively manage risk, and clarify responsibilities. By August 30, 2013, request you provide a point of contact (POC) to coordinate implementation of the following:

- The DoD Chief Information Officer (DoD CIO) will establish a Memorandum of Agreement (MOA) with each Federal Department and Agency requiring connection to the DoD SIPRNET. The DoD CIO will provide a draft MOA for each Federal Department and Agency, as well as their DoD Component sponsor of record. Each MOA will identify and assign responsibilities to the DoD CIO, the DoD Component sponsor, and the Federal Department or Agency to ensure connections to the SIPRNET are mission essential, properly maintained and defended at all times. Applicable Committee for National Security Systems

(CNSS) and SIPRNET personnel, cyber and physical security requirements will be included in each MOA. The goal is to complete MOAs with all Federal Departments and Agencies by 2QFY14.

- All Federal Department and Agency connections to the SIPRNET will be made via the SIPRNET Federal Demilitarized Zone (SIPRNET FED DMZ). For those Federal organizations that do not connect through the SIPRNET FED DMZ, the Defense Information Systems Agency will collaborate with the respective organizations to develop a plan of action and milestones to move each connection to the SIPRNET FED DMZ. The migration will be reflected in the MOAs and funded by each of the Federal Departments and Agencies.

Please provide POC information to Mr. Al Johnson, roy.a.johnson22.civ@mail.mil, 703-692-9240; and Mr. Thomas N. Orme, thomas.n.orme.civ@mail.mil, 571-372-4431. We look forward to working with you on this effort.


Teresa M. Takai

cc:

Under Secretary of Defense for Policy
Under Secretary of Defense for Intelligence
United States Strategic Command, J6
Commander, United States Cyber Command
United States Transportation Command, J6
United States Northern Command, N-NC/IC
United States Air Force Space Command, A6
Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
Director, Defense Technology Security Administration
Director, Defense Information Systems Agency
Chief Information Officer, DoD Inspector General
Chief Information Officer, Defense Intelligence Agency
Chief Information Officer, National Security Agency
Chief Information Officer, Joint Staff
Chief Information Officer, Department of Commerce
Chief Information Officer, Department of Energy/National Nuclear Security Administration
Chief Information Officer, Department of Homeland Security