OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

AUG 16 2016

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHIEFS OF THE MILITARY SERVICES

SUBJECT: Operational Testing of Joint Regional Security Stacks (JRSSs)

Reference: Joint Interoperability Test Command (JITC), "Joint Regional Security Stack Initial Operational Assessment Phase 2 Report (U)," April 2016

I placed the Joint Information Environment (JIE) on operational test oversight because of its broad potential to affect the effectiveness, suitability, and cybersecurity of DOD information networks. I am concerned that the Services are choosing to field JRSS, a critical core enabling capability of JIE, as part of a schedule-driven approach and without the operational test and evaluation necessary to determine whether the JRSS is operationally effective, operationally suitable, and secure against cyber attacks. The Army has already fielded JRSS to select locations (although it still wisely relies on legacy security stacks for cyber defense), the Air Force plans to migrate to JRSS starting in September 2016, and the Navy also plans to migrate to JRSS in the future. There has been no operational test and evaluation of JRSS.

Acquiring and deploying the JRSS without operational testing significantly increases risks to the missions and forces which rely on the affected networks. The limited early test data reported by JITC in April 2016 (see reference) shows that JRSS capabilities are immature, lacking a stable configuration, and that operator training is incomplete and insufficient. Of most concern is JITC's finding that key JRSS cybersecurity functions are not mission capable.

The procedures for operation, defense, and management of JRSSs within DOD networks fundamentally differ from legacy procedures, and new procedures have yet to be developed. Fielding JRSSs prior to operational testing to ensure the technology works, and that network operators and defenders have effective procedures and training, risks degrading network operations and security, and could leave networks vulnerable to undetected adversarial actions after JRSS migration.

I strongly recommend that the Services conduct rigorous and comprehensive operational test and evaluation of the JRSS capability prior to fielding, and in particular prior to relying on JRSS for network security. I further recommend that the Services consider the results of operational testing in their fielding decisions.

My staff is ready to support the development of JRSS operational test plans for my approval, tailored to each Service.

J. Michael Gilmore
Director

cc:
Chief Information Officer, DOD
Director, Defense Information Systems Agency
Director for Command, Control, Communications and Computers/Cyber, J6 and Chief Information Officer, Joint Staff
Chief Information Officer/G-6, Army
Chief Information Officer, Navy
Chief Information Dominance and Chief Information Officer, Air Force
Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, Acquisition, Technology and Logistics, OSD
Commander, Air Force Operational Test and Evaluation Center
Commander, Army Test and Evaluation Command
Commander, Operational Test and Evaluation Force
Commander, Joint Interoperability Test Command