**DEPARTMENT OF DEFENSE**
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

OCT 06 2014

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Wireless Peripherals Guidance

References: (a) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as amended

(b) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

This memorandum provides clarification of References (a) and (b) on the use of wireless peripherals, such as wireless keyboards, mice, and presentation controllers, for computing devices in non-tactical applications within the Department of Defense (DoD) enterprise. Wireless devices and peripherals that connect to DoD networks are part of those networks and must be configured and managed in accordance with the cognizant Authorizing Official's (AO) Authority to Operate, the Risk Management Framework (Reference (b)), and applicable Defense Information Systems Agency Security Technical Implementation Guides.

Reference (a) establishes a number of security requirements with regards to wireless systems (e.g., strong authentication, non-repudiation, encryption, etc). However, in accordance with References (a) and (b), exceptions may be granted on a case-by-case basis as determined by the AO for the wireless connections under their control.

In order to demonstrate sufficient due diligence and document mitigations for use of wireless peripherals, the following measures shall be considered:

- Develop and calculate risk for the particular product based on mission or organizational risk tolerances in accordance with References (a) and (b).
- Consider product risks in the context of the specific operational use environment.
- Mitigate risks with documented tactics, techniques, and procedures. Introduce additional user training specific to the wireless peripheral.
- Document residual risk and vulnerabilities in the system Plan of Action & Milestone.
- Ensure proper implementation of the product by the Information System Owner in coordination with the Information System Security Officer and Information System Security Manager.

The point of contact for this matter is Mr. Mark Norton, 571-372-4941, mark.c.norton.civ@mail.mil.

Terry A. Halvorsen
Acting