



31 MAR 2014

MEMORANDUM FOR: SEE DISTRIBUTION

Subject: Effective Integration of Cyber and Traditional Security Efforts

- References:
- (a) DoD Directive 5200.43, *Defense Security Enterprise*, October 1, 2012
 - (b) DoD Manual 5200.01, *DoD Information Security Program: Protection of Classified Information*, Volume 3, February 2, 2012
 - (c) DoD Regulation 5200.02, *Personnel Security Program*, January 1, 1987
 - (d) DoD Regulation 5200.8-R, *Physical Security Program*, September 4, 2007
 - (e) DoD Directive 8500.01E, *Information Assurance*, October 24, 2002
 - (f) DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003
 - (g) Chairman Joint Chiefs of Staff Instruction 6510.1F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, February 9, 2011
 - (h) CJCS EXORD for USSTRATCOM, DTG 112050Z, Feb 11
 - (i) USSTRATCOM OPOD Operation Gladiator Phoenix, DTG 182216Z Feb 11

DoD is the world's largest user of information technology. It is also the principle creator of classified information in the U.S. government; much of which is hosted on thousands of networks worldwide. It is imperative that we recognize and address the risk posed by emerging and constantly evolving threats to our data-centric capabilities, and pursue an enhanced information protection approach and partnership that results in unity of security efforts to secure our networks, facilities, personnel, and operations while minimizing the insider threat. To this end, the Under Secretary of Defense for Intelligence (USD(I)), the DoD Chief Information Officer (DoD CIO), and the Commander, United States Strategic Command (CDRUSSTRATCOM) will work together to ensure:

- Development of an enterprise-level approach, consistent with reference (a), to achieve alignment and integration of security requirements for inspection and oversight of Component traditional (Information, Personnel, Physical, and Industrial) and Information Assurance (IA) security programs during the conduct of Command Cyber Readiness Inspections (CCRIs) as detailed in reference (g).
- Joint development and promulgation of revised CCRI processes that provide a broad assessment of a Command's security posture incorporating traditional and cybersecurity guidelines, as set forth in references (a) through (e), using a risk management approach.
- Development and promulgation of any necessary policy changes in references (b) through (e) to address: granting inspection authorities for execution of CCRIs by joint or combined teams of traditional and IA security professionals; the process for allocating limited security resources while giving due consideration for risk

management principles in a manner that results in informed decision making by Component leadership; and adoption of any additional methodologies to avoid mission failure, catastrophic loss of information, or loss of data-centric capabilities.

- Expand the CCRI program to include assessing the physical security and IA of supervisory control and data acquisition (SCADA) and Voice Over IP (VOIP) networks and systems for targeted, emerging, and constantly evolving threats.
- Review and alignment of the Cyber Security Inspection Program outlined in references (h) and (i), for the purpose of achieving effective integration of traditional (Information, Personnel, Physical, and Industrial) and IA programs when conducting CCRIs, following the policy guidance provided in references (a) through (f).

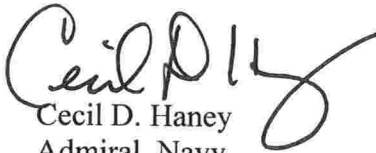
Our points of contact for this initiative are Mr. Timothy Davis, OUSD(I) at (703) 607-0089, Mr. Richard Hale, DoD CIO at (703) 695-8705, and Ms. Kerry Kelley, USSTRATCOM/J6 at (402) 294-5691.



Teresa M. Takai
Department of Defense,
Chief Information Officer



Michael G. Vickers
Under Secretary of Defense
for Intelligence



Cecil D. Haney
Admiral, Navy
Commander
United States Strategic Command

DISTRIBUTION:

**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
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES**