DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

DEC 2 2011

SAIS-CB

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Developing Information Technology Contingency Plans

1. References:

a. Army Regulation (AR) 25-2, Information Assurance, 23 March 2009.

b. Information Assurance Best Business Practice (IA BBP) 08-CO-M-0001, U.S. Army CIO/G-6, Cyber Directorate, 7 September 2001, subject: Information Technology Contingency Plans and Testing, Version 1.2.

c. Department of the Army Pamphlet 25-1-2, Information Technology Contingency Planning, 16 November 2006.

2. This interim policy memorandum directs all Army organizations to develop and maintain an Information Technology Contingency Plan (ITCP) for each Information System (IS) as determined by risk assessments. The ITCPs shall be developed in accordance with Public Law, the Federal Information Security Management Act of 2002 (FISMA), Department of Defense (DoD) Directives and Army Regulations.

3. An ITCP details emergency responses, backup operations, transfer of operations, and post-disaster recovery procedures that would be implemented during a major disruption of IS service. Do not confuse the ITCP with a Continuity of Operations Plan, which provides procedures to sustain an organization's essential functions. Detailed guidance for developing an ITCP is provided in the ITCP BBP, which can be retrieved from the Cyber Directorate Information Assurance Portal, https://www.milsuite.mil/wiki/Best_Business_Practices.

4. This interim policy memorandum delineates responsibilities for ensuring that an organization has a properly completed ITCP for each IS.

a. The System Owner (SO) is a Government civilian or military person or organization. The SO has the overall responsibility to ensure that an ITCP is

developed, maintained, and tested for each IS in accordance with National, DoD and Army requirements.

b. Information technology contingency planning is also a command responsibility. Commanders, senior executives, program executive officers, and directors must establish an ITCP policy and appoint a properly trained ITCP Coordinator.

5. This interim policy memorandum is effective on 1 December 2011. Changes will be codified in the next revision of AR 25-2.

6. The point of contact for this interim policy memorandum is Ms. Melissa Hicks, (703) 545-1604, melissa.c.hicks.civ@mail.mil.

Susan S. Lawrence
SUSAN S. LAWRENCE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER
U.S. ARMY FORCES COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY EUROPE AND SEVENTH ARMY
U.S. ARMY CENTRAL
U.S. ARMY NORTH
U.S. ARMY SOUTH
U.S. ARMY AFRICA
U.S. ARMY PACIFIC
U.S. ARMY CYBER
U.S. ARMY SPECIAL OPERATIONS COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC COMMAND

COMMANDER
U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND (ARMY)
(CONT)

DISTRIBUTION: (CONT)
U.S. ARMY MEDICAL COMMAND
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY CORPS OF ENGINEERS
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY TEST AND EVALUATION COMMAND
U.S. ARMY RESERVE COMMAND
U.S. ARMY INSTALLATION MANAGEMENT COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY
DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER