DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 300-50-8*

MAY 0 2 2014

# POLICIES

## Continuity Program

1. **Purpose.** This Instruction prescribes policy and assigns responsibilities for the Continuity Program for DISA.

2. **Applicability.** This Instruction applies to all DISA activities.

3. **Authority.** This Instruction is published in accordance with the authority contained in DoD Directive 3020.26, Department of Defense Continuity Programs (DCP), 9 January 2009.

4. **Reference.** DoD Instruction 3020.42, Defense Continuity Plan Development, 17 February 2006.

5. **Definitions.** Definitions are provided in the enclosure.

6. **Background.** National, Executive Branch, and DoD policy require a comprehensive and effective program to ensure survival of our constitutional form of government and continuity of national essential functions under all circumstances. This involves continuity of operations (COOP) capabilities maintained at a high level of readiness and the ability to implement plans both with and without warning. The evolving threat environment has increased the need for organizational COOP capabilities, plans, and preparedness to continue mission essential functions (MEFs) across the spectrum of emergencies. An organization's resiliency is directly related to the effectiveness of its continuity capability. Effective continuity programs and plans require a coordinated, cross-functional approach to planning and preparedness. COOP planning and capabilities require and are supported by related business continuity planning and information technology (IT) contingency planning.

7. **Policy.**

7.1 A coherent, comprehensive, and capable continuity program will be maintained by the Agency to ensure the performance of MEFs continue across the "all hazards" spectrum of threats and emergencies. Continuity requirements will be incorporated into the daily operations of all organizations to ensure seamless and immediate continuation of MEFs during any emergency including localized acts of nature, accidents, and technological or attack-related emergencies. COOP planners should assume they will have no warning. Continuity planning will occur simultaneously with development and execution of DISA programs. Organizations will incorporate redundancy and resiliency as a means and an end.

7.2 According to the authority and reference document, minimum continuity program elements will be operations orders (OPORDs), plans, and procedures that delineate essential functions; specify orders of succession to office and emergency delegations of authority; identify a range of continuity facilities and locations; provide for the identification, safekeeping, and accessibility of vital records, files, and databases; provide for interoperable communications; provide for human capital planning and preparedness; validate continuity capabilities through test, training, and exercise (TT&E); specify a devolution of control and direction; and provide for recovery and subsequent reconstitution. Continuity of MEFs during a threat or emergency event will be the basis for organizational continuity planning, preparation, and execution.

7.3 Resources will be planned, programmed, and budgeted to meet continuity program policies and requirements.

7.4 The continuity program will maximize use of technological solutions to provide information to leaders and other users, facilitate decisionmaking, maintain situational awareness, and issue orders and direction to support continuity of MEFs during and following an emergency.

7.5 Alternate facility selection will include critical infrastructure assessment, facility vulnerability assessment, and risk analysis vetted by the senior official or officials responsible for selecting or operating at the alternate facility. Provisions will be made for the availability and redundancy of critical communications capabilities at alternate and devolution facilities commensurate with the execution requirements of MEFs performed in order to support connectivity between and among key government leadership, DoD leadership, DoD Components, and other critical Departments, Agencies, and mission partners.

8. **Objective.** The objective of the Continuity Program is to ensure the continuation of MEFs supporting the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, DoD Components, and mission partners under all circumstances.

9. **Oversight and Delegation of Authority.** Oversight responsibilities for the Heads of the DoD Components are delineated in DoD Directive (DoDD) 3020.26 (authority document) and DoD Instruction 3020.42 (reference document). The Director, DISA, delegates authority in this Instruction.

10. **Responsibilities.**

10.1 **Principal Director for Operations (OP).** The Principal Director, OP, serves as the senior official accountable to the Director, DISA, for oversight of the Continuity Program to ensure program management, policy, planning, preparedness, allocation of resources, and compliance with DoD continuity guidance, directives, strategy, and standards. The Principal Director, OP, may further delegate authority for parts of the Continuity Program to other DISA offices, as appropriate, but may not delegate the responsibility. The Principal Director, OP, will:

10.1.1 Conduct periodic Continuity Program in-progress reviews (IPRs), at least annually, to support program requirement validation and the budget development process. The IPR should consider the status of program elements, continuity capabilities and vulnerabilities, day-to-day readiness, funding and allocation of resources, and status of lessons learned from exercises and actual emergency events.

10.1.2 Ensure COOP plans and OPORDs are coordinated with complementary and supporting programs, plans, and offices; such as, critical infrastructure, information assurance, business continuity and IT contingency planning, facility occupant emergency planning, antiterrorism, and crisis management.

10.1.3 Provide a focal point for the Continuity Program and official point of contact for internal and external organizations for coordinating COOP issues and activities and organizational continuity hardware and software requirements.

10.1.4 Provide program management, policy, planning, operational execution of plans and TT&E programs consistent with DoD guidance and directives, to include a corrective action program (CAP) to assist in documenting, prioritizing, and resourcing continuity issues identified from TT&E lessons learned, evaluations, assessments, and emergency operations.

10.1.5 Designate a Continuity Program Manager.

10.2 **Principal Director for Network Services (NS).** The Principal Director, NS, ensures continuity capabilities of network operations including operational support systems and Defense Information Systems Network (DISN) management to maintain voice, video, data networks, and other network capabilities, as they transfer to sustainment under NS. In addition, ensure strategic mission support to ensure continuity of MEFs under all threat and emergency situations.

10.3 **Director for Manpower, Personnel, and Security (MPS).** The Director, MPS, will:

10.3.1 Ensure policy, processes, and procedures for personnel accountability for DISA organizations worldwide address accountability challenges during a COOP contingency.

10.3.2 Develop policy for activating an incident management team (IMT) and supporting emergency preparedness plans to support the Senior Leader Decision Group (SLDG) through the DISA Command Center (DCC) during an emergency event affecting a DISA facility that could lead to a decision to execute COOP.

10.3.3 Provide facility reconstitution and associated logistics support to ensure continuity of MEFs following a COOP event.

10.3.4 Develop emergency preparedness plans and procedures complementary to COOP execution; such as, security, evacuation, and antiterrorism.

10.4 **Chief Information Officer (CIO).** The CIO will:

10.4.1 Validate organizational continuity hardware and software requirements, in conjunction with OP.

10.4.2 Plan, implement, and maintain communication infrastructures for systems and networks at COOP locations, as assigned.

10.4.3 Manage, provide, and maintain administrative voice systems and wireless services for COOP at DISA headquarters (HQ).

10.4.4 Provide MEF-related data replication on the DISANet for designated alternate sites and support for COOP reconstitution efforts.

10.4.5 Provide personnel to support alternate sites during training, exercise, and actual events.

10.5 **Director for Procurement/Defense Information Technology Contracting Organization (DITCO) (PLD).** The Director, PLD, will:

10.5.1 Ensure identification and backup of vital contracting and acquisition records, files, and databases having such value that their loss would prevent or significantly impair the execution of MEFs during a COOP contingency.

10.5.2 Develop provisions for the acquisition of resources and services necessary for continuity of MEFs during and after COOP contingencies affecting any DISA facility worldwide.

10.6 **Director for Strategic Planning and Information (SPI).** The Director, SPI, will:

10.6.1 Provide planning advice to OP for the Continuity Program, as required.

10.6.2 Develop Agency public affairs policy concerning continuity activities and actions planned or implemented in response to threats and emergency events at DISA facilities worldwide.

10.6.3 Provide senior DISA leaders with recommended courses of action for public affairs support of COOP contingencies.

10.7 **General Counsel (GC).** The GC will review Continuity Program policy and plans and provide legal counsel, as appropriate, prior to distribution and implementation.

10.8 **Chief Financial Executive/Comptroller (CFE).** The CFE will:

10.8.1 Provide programming and budget development advice to OP for the Continuity Program, as required.

10.8.2 Coordinate with OP and CIO to develop policy, processes, and guidance for organizations to report continuity-related budget execution and program funding to support periodic reviews from the Office of the Secretary of Defense, as required.

10.9 **Chief of Staff (COS).** The COS will maintain coordination and liaison with U.S. Cyber Command (USCYBERCOM) and U.S. Strategic Command (USSTRATCOM) concerning the Continuity Program and DISA-wide continuity plans, as appropriate.

10.10 **Principal Directors, Directors, Chiefs, and Commanders of Major Organizational Elements.** These individuals will:

10.10.1 Develop, coordinate, and maintain organizational COOP OPORDs or plans and validate, update, and reissue the documents every 2 years, or more frequently as changes warrant, in accordance with the DoDD 3020.26 (authority document). (DISA HQ directorates will not duplicate planning or content of the DISA HQ COOP OPORD.)

10.10.2 Review, validate, and prioritize organizational MEFs every year, or more frequently as changes warrant, to include identification of internal and external interdependencies that are part of or influence each MEF.

10.10.3 Identify vital files, records, and databases, including classified or sensitive data, and information systems, software, and hardware which are necessary to perform essential functions and activities, to include the backup, safeguarding, availability, and accessibility of the data to support continuity operations.

10.10.4 Ensure all organizational personnel complete annual continuity awareness training.

10.10.5 Ensure all organizational personnel who are assigned to activate, support, host, or sustain continuity operations, as well those designated as members of the Emergency Relocation Group (ERG) or subject matter experts (SMEs) are trained concerning their part in COOP and related contingency plans and execution of MEFs.

10.10.6 Integrate operations security (OPSEC) requirements into continuity planning, training, execution, and operations.

10.10.7 Ensure organizational COOP-related documentation and communications including plans, reports, messages, e-mails, and phone conversations are properly classified and appropriate safeguards are implemented to protect COOP documents, in accordance with the DoD Defense Continuity Program (DCP) Security Classification Guide, 15 December 2005. (A copy of the guide is available in the Operations Directorate (OP) Plans, Exercises, and Readiness Division (OP5) COOP Branch (OP51). The guide is also located on the DISA COOP Web site accessible by the directorate Emergency Planning Coordinators on the Secret Internet Protocol Router Network.)

10.10.8 Advise CFE and OP of funding shortfalls that would prevent effective operations and maintenance of existing systems or prevent or delay scheduled implementation of new subsystems or projects required for COOP capabilities and readiness.

10.10.9 Provide copies of organizational COOP OPORDs or plans to the OP Plans, Exercises, and Readiness Division (OP5) COOP Branch (OP51).

10.11 **Commanders of DISA NetOps Centers (DNCs), Commanders of DISA Field Offices, and Chiefs and Commanders of Defense Enterprise Computing Centers (DECCs).** These individuals will:

10.11.1 Develop an organizational COOP OPORD or plan including related operating plans, procedures, and checklists, consistent with DoD and DISA planning guidance, to ensure continuity of organizational MEFs and critical networks.

10.11.2 Support COOP TT&E program requirements and notify OP of any locally planned COOP exercises to enable integration of objectives, planning support, and synchronization of events.

10.11.3 Coordinate COOP OPORDs or plans with the DISA Command Center (DCC) and the impacted DNCs and the supported combatant command, as applicable.

10.12. **Continuity Program Manager Duties.** The Continuity Program Manager will:

10.12.1 Manage and coordinate allocation of COOP program resources.

10.12.2 Develop an Agency-wide continuity program policy and concept of operations.

10.12.3 Develop HQ-specific continuity policy and guidance.

10.12.4 Provide guidance to organizations on analysis, periodic review, and validation of continuity MEFs, to include hardware and software requirements, and coordinate, validate, and leverage these efforts with CIO analysis of mission essential tasks, as applicable.

10.12.5 Provide a central repository for Agency organizational COOP OPORDs and plans.

10.12.6 Coordinate with the DCC concerning the Continuity Program and DISA-wide plans and operations, as appropriate.

10.12.7 Provide continuity awareness training for the DISA workforce.

10.12.8 Provide initial and recurring COOP training for DISA HQ organizational personnel who are assigned to activate, support, host, or sustain continuity operations, as well as those designated as ERG members or SMEs. In addition, assist non-HQ DISA organizations in developing their own recurring training.

11. **COOP Operations Orders and Plans.**

11.1 The content of a COOP OPORD or plan is flexible and should address identification of organizational essential functions that must be maintained in a continuity event; a concept of operation that describes how the essential functions will be accomplished to include devolution of technologies and or relocation strategies, ERG members, alert and notification procedures; orders of succession; emergency delegations of authority for designated positions; the location and description of continuity facilities; a vital records program that ensures safekeeping and the accessibility of key data; and a process for organizational recovery or reconstitution.

11.2 OPORDS or plans should also accomplish the following:

11.2.1 Be responsive and executable during duty and nonduty hours, with or without warning, and provide essential operational capability within a minimum acceptable period of disruption for MEFs including essential command and control (C2) and core support functions, but in all cases within 12 hours of COOP plan activation, and provide the capability to sustain operations until normal business activities can be resumed or reconstituted, which may be up to 30 days and beyond.

11.2.2 Be supported by other business continuity plans and IT contingency plans, as needed, to ensure continuity of MEFs.

11.2.3 Leverage existing complementary programs, plans, and procedures; such as, those associated with crisis management, occupant emergencies, information assurance, antiterrorism, incident response and consequence mitigation plans, and installation preparedness.

11.2.4 Be exercised annually, or as otherwise directed, to evaluate and validate program readiness, as required by the authority document.

11.2.5 Be coordinated with supported organizations, application owners, and host organizations, as applicable.

Enclosure a/s

FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES. This revision incorporates reorganizations within DISA HQ and realignments of responsibilities within DISA directorates.

*This Instruction replaces DISAI 300-50-8, 24 October 2008, and must be reissued, canceled, or certified current within 5 years of its publication. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.
OPR: OP - disa.meade.gig-op.mbx.coop@mail.mil
DISTRIBUTION: P