



Department of Defense INSTRUCTION

NUMBER 3020.39

August 3, 2001

ASD(C3I)

SUBJECT: Integrated Continuity Planning for Defense Intelligence

- References:
- (a) [DoD Directive 3020.36](#), "Assignment of National Security Emergency Preparedness (NSEP) Responsibilities to DoD Components," November 2, 1988
 - (b) [DoD Directive 3020.26](#), "Continuity of Operations (COOP) Policy and Planning," May 26, 1995
 - (c) [DoD Directive 5137.1](#), "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992
 - (d) [DoD 8910.1-M](#), "DoD Procedures for Management of Information Requirements," June 30, 1998
 - (e) DoD Directive S-3600.1, "Information Operations (IO) (U)," December 9, 1996

1. PURPOSE

1.1. This Instruction implements policy and assigns responsibilities to the DoD Components to carry out integrated continuity planning for Intelligence functions under the authorities in reference (a).

1.2. It amplifies guidance in references (a) and (b) to ensure that:

1.2.1. Business continuity planning, which includes Information Technology (IT) disaster recovery planning, supports and supplements National Security Emergency Preparedness and Continuity of Operations (COOP) planning.

1.2.2. All continuity planning builds upon any assessments developed by the Critical Infrastructure Protection (CIP) and Information Assurance (IA) programs and

integrates, where applicable, with any response mechanisms, reporting requirements, or other procedures related to those programs.

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred collectively to as "the DoD Components").

2.2. This Instruction particularly applies to the Defense Intelligence Agency (DIA), the National Imagery and Mapping Agency (NIMA), the National Reconnaissance Office (NRO), the National Security Agency/Central Security Service (NSA/CSS), and to the Defense Information Systems Agency (DISA).

2.3. Continuity planning includes all planning related to maintaining or recovering functional capabilities before, during, and after disruptions. This includes business/operational continuity planning, CIP and IA planning, COOP planning, IT disaster recovery planning, emergency/disaster preparedness planning, and any other planning related to maintaining the capability to conduct organizational functions before, during, and after disruptions.

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. Each DoD Component shall plan for survival, recovery, and reconstitution of its mission-essential functions.

4.2. DoD intelligence capabilities are particularly critical to making decisions and operating the Armed Forces.

4.3. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall, according to reference (a), provide policy guidance and support for intelligence activities, including preparedness planning and

programming, within the Department of Defense for survivability of intelligence capabilities. The ASD(C3I) shall also, according with reference (c), establish policy and provide direction to the DoD Components on all matters concerning intelligence programs, systems, and equipment.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for intelligence matters, and in consultation with the Office of the Director of Central Intelligence (DCI), as appropriate, shall:

5.1.1. Oversee continuity planning for intelligence functions within and among the DoD Components to ensure it accords with reference (a) and this Instruction.

5.1.2. Develop a program to periodically assess the readiness of the Intelligence continuity programs of the DoD Components according to this Instruction.

5.1.3. Ensure DIA, NIMA, NRO, and NSA work together to:

5.1.3.1. Based on essential functions, prioritize defense intelligence products and services and develop a dynamic process to continue the delivery of products and services consistent with those priorities.

5.1.3.2. Conduct special exercises and/or evaluate operations with an interagency emphasis regularly to ensure that continuity plans are complete and viable.

5.1.4. Prepare, based on DIA, NIMA, NRO, and NSA input discussed in subparagraph 5.3.10. of this Instruction, an annual report that:

5.1.4.1. Assesses the overall status of defense intelligence integrated continuity planning.

5.1.4.2. Determines courses of action to correct deficiencies.

5.1.4.3. Advocates resource and funding alternatives.

5.1.4.4. Is available to the Office of the DCI, the Under Secretary of Defense (Policy), and all DoD Components with intelligence functions.

5.2. The Secretaries of the Military Departments and the Combatant Commanders shall plan for survival, recovery, and reconstitution of their mission-essential

intelligence functions and, as appropriate, coordinate with the Directors of DIA, NIMA, NSA, and NRO on those actions or activities described in paragraph 5.3., below.

5.3. The Directors of the Defense Intelligence Agency, the National Imagery and Mapping Agency, the National Reconnaissance Office, and the National Security Agency shall comply with this Instruction by developing an integrated continuity planning program for their functions that, at a minimum:

5.3.1. Integrates and coordinates planning for COOP, operational or functional continuity, IT disaster recovery, emergency/disaster preparedness, CIP and IA programs, and any other planning related to maintaining mission-essential functions. This integrated continuity planning program shall:

5.3.1.1. Be a part of an overall strategy to protect defense intelligence capabilities, respond adequately to man-made or environmental threats or contingencies, and maintain mission-essential functions through sound risk-management and funding decisions.

5.3.1.2. Ensure coordination at intra-agency and interagency planning levels.

5.3.1.3. In coordination with the Office of the DCI, plan for and identify adequate resources and assets to ensure that their Component can execute planned actions. To the extent practicable, this planning should rely upon existing assets and shared resources rather than resources to be procured at the time of plan execution.

5.3.2. Establishes and maintains a listing or database that shall:

5.3.2.1. Identify and prioritize all mission-essential functions, distinguishing those that must be restored within 12 hours after a national security emergency from those that can be deferred until time and resources permit restoration. Prioritization processes will adapt to emerging conditions during times of peak demand and disruptions. This listing will be based on customer input and coordination among DoD Components with intelligence functions.

5.3.2.2. Identify the cyber and physical assets and personnel essential to conducting, developing, and delivering intelligence products and services for the above mission-essential functions.

5.3.3. Develops a common process for all continuity plans and activities to continuously monitor situations, evaluate disruptions, and enable prudent decision-making.

5.3.4. Integrates risk analysis, hazard identification, and vulnerability assessments (including CIP assessments) and uses this information in all continuity planning.

5.3.5. Develops, exercises, and refines continuity plans integral to normal operational planning, standard management practice, and overall funding strategies.

5.3.6. Develops training and exercise procedures and activities that are regularly rehearsed and tested and that shall benefit multiple continuity planning requirements (e.g., using an emergency drill to initiate a continuity plan exercise).

5.3.7. Plans for backing up and restoring all systems and networks (including local area networks) that support mission-essential functions.

5.3.8. Coordinates with defense intelligence customers and suppliers to ensure that continuity plans are complete, coherent, and meet customer needs.

5.3.9. Maintains continuity planning funding data to assist the Component in identifying shortfalls.

5.3.10. Provides an annual report on the status of exercises and operational evaluations of continuity plans to ASD(C3I) and the Office of the DCI, beginning October 2001. Reports shall identify shortcomings, highlight successful practices, and identify plans for remedying shortcomings during the upcoming year.

5.4. The Director, Defense Information Systems Agency, shall support intelligence continuity planning programs by:

5.4.1. Providing representation and appropriate expertise on DISA-related communications functions to any continuity planning teams working on mission-essential intelligence functions dependent on DISA services.

5.4.2. Assisting the Components in developing appropriate work-arounds should failures disable normal telecommunications channels used for intelligence functions. Continuity planning and restoration of non-DISA-provided telecommunications services will be on a reimbursable (Defense Working Capital Fund) basis.

5.4.3. Supporting, or participating in, as appropriate, interagency continuity planning training and exercises.

6. INFORMATION REQUIREMENTS

Intelligence continuity plans, including all response mechanisms and reporting requirements referred to in this Instruction, are exempt from licensing in accordance with paragraphs C4.4.2. - C4.4.4., DoD 8910.1-M (reference (d)).

7. EFFECTIVE DATE

This Instruction is effective immediately.



**Acting Assistant Secretary of Defense
(Command, Control, Communications,
and Intelligence)**

Enclosures - 1

E1. Definitions

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Business Continuity Planning (BCP). As it applies to the Defense Intelligence Components, BCP focuses on the Component's ability to continue or quickly recover its mission-essential functions following any disruption short of a major catastrophe or national security emergency. BCP may be incorporated into a specific plan or, when appropriate, in documents such as standard operating procedures, and generally are distributed widely so that all relevant personnel are familiar with the required procedures and associated responsibilities.

E1.1.2. Continuity of Operations (COOP) Planning. As it applies to the Defense Intelligence Components, it focuses on the Component's ability to continue mission-essential functions without unacceptable interruption in situations such as catastrophes or national security emergencies. It includes preparatory measures, response actions, and restoration activities that ensure these functions continue to maintain military effectiveness, readiness, and survivability. COOP planning designates mission-essential functions and essential personnel, alternate headquarters and work sites, and alternate processes for conducting mission-essential functions from these work sites.

E1.1.3. Continuity Planning. An umbrella term for planning the continuity of organizational operational and business functions should disruptions occur due to natural disasters, man-made causes (unintentional and deliberate actions), or technological failures. This "all-hazards" planning focuses on the actions necessary to continue mission-essential and other functions, rather than on why the disruption occurred. Types of Continuity Planning include:

E1.1.3.1. Business Continuity Planning (BCP).

E1.1.3.2. Continuity of Operations (COOP) Planning.

E1.1.3.3. IT Disaster Recovery Planning.

E1.1.3.4. Emergency Planning.

E1.1.3.5. Disaster Planning.

E1.1.3.6. Other types of planning activities and programs that shall be integrated into Continuity Planning include:

E1.1.3.6.1. Critical Infrastructure Protection.

E1.1.3.6.2. Information Assurance.

E1.1.4. Critical Infrastructure Protection. The identification, assessment, and assurance of cyber and physical infrastructures that support mission-critical capabilities and requirements, to include the political, economic, technological, and information security environments essential to the execution of the National Military Strategy.

E1.1.5. Disaster Planning. Procedures for storms, earthquakes, and other natural disasters. Most often used conducting mitigating actions, such as evacuations, when warning conditions exist.

E1.1.6. Emergency Planning. Procedures for fires, bomb threats, hazardous material releases, etc., which deal with how emergency response is conducted at a particular work site.

E1.1.7. Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: DoD Directive S-3600.1 (reference (e)).) Additionally, Information Assurance programs require the entire information infrastructure to have reconstitution procedures for critical assets and systems operations.

E1.1.8. Integrated Continuity Planning. A process by which continuity planning management, funding, products, services, and activities are coordinated, mutually supported, and based on common assessments, assumptions, and resource listings.

E1.1.9. IT Disaster Recovery Planning. A process that focuses on data/computing center and/or local/wide area network recovery following a disruption including specific actions for restoring or recovering IT and other systems after they fail. These plans usually include the procedures to safeguard information by conducting backups or similar procedures to permit the restoration of information. These plans are prepared by system administrators, but include appropriate links to the business continuity plans of all functions that rely on that system or IT component. (See also Information Assurance.)

E1.1.10. Mission-Essential Functions. They include those functions that must be performed without unacceptable interruption to achieve the Component's critical missions, and include:

E1.1.10.1. Command and control of assets.

E1.1.10.2. Receiving, assessing, analyzing, processing, displaying, and disseminating information necessary to perform critical missions and support decision making.

E1.1.10.3. Performing other operations that must be performed to achieve mission success. (Source: Reference (b).)