TABLE OF CONTENTS
IT CONTINGENCY PLANNING
DM 3570-000

U.S. Department of Agriculture
Washington, D.C.

DEPARTMENTAL MANUAL	NUMBER: 3570-000
SUBJECT: IT Contingency and Disaster Planning	DATE: February 17, 2005
	OPI: Office of the Chief Information Officer, Cyber Security

CHAPTER 14
GENERAL INFORMATION

1 PURPOSE

The purpose of this Departmental Manual chapter is to provide the requirements for Information Technology (IT) Contingency Planning to U. S. Department of Agriculture (USDA) agencies and staff offices. This type of planning is necessary to ensure that IT mission critical systems and sensitive systems continue to be operational in the event of major or minor interruptions or a large-scale disaster. Use of formal Contingency and Disaster Recovery Plans also ensures that USDA agencies and staff offices have effective and efficient recovery solutions for their systems.

IT Contingency Planning includes activities designed to recover and sustain critical IT services following an emergency. These arrangements fit into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. The focus of Part 1 of this chapter is the preparation, testing, and maintenance of the Disaster Recovery Plan (DRP) and Business Resumption Plan (BRP).

2 CANCELLATION

This Departmental Manual chapter will be in effect until superseded.

3 REFERENCES

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources", Appendix III;

E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. 3531 et seq.;

Homeland Security Directive HSPD-7, Critical Infrastructure Identification, Prioritization and Protection;

Presidential Decision Directive (PDD) 67: Enduring Constitutional Government and Continuity of Government, October 1998;

Federal Preparedness Circular (FPC) 65: Federal Executive Branch Continuity of Operations, July 1999;

Federal Emergency Management Agency (FEMA) Federal Response Plan (FRP); April 1999;

National Institute of Standards and Technology (NIST) Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems"

4 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees and other activities.

5 ABBREVIATIONS

BIA	Business Impact Analysis
BRP	Business Resumption Plan
BCP	Business Continuity Plan
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations Plan
CS	Cyber Security
DRP	Disaster Recovery Plan
GAO	General Accounting Office
IRM	Information Resources Management
IT	Information Technology

OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
USDA	United States Department of Agriculture

6 DEFINITIONS

a Back-up Site (Alternate Site) – a facility that is able to support system operations in restoring critical systems to an acceptable level as defined in the DR plan. Sites are referred to as: cold, warm, hot, mobile, and mirrored.

b Business Impact Analysis (BIA) - An analysis of the business processes and interdependencies used to characterize contingency requirements and priorities in the event of a significant disruption of service. More information concerning the BIA can be found in NIST Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems.

c Contingency Planning – Refers to the dynamic development of a coordinated recovery strategy for IT systems or application, operations, and data after a disruption. The planning process requires several steps: develop policy; conduct business impact analysis (BIA); identify preventive controls; develop recovery strategies; develop contingency plan; test and exercise the plan; train personnel; and maintain the plan.

d Contingency Planning Coordinator - designates appropriate teams to implement the recovery strategy. Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation.

e Disruption – An unplanned event that causes the General Support System or Major Application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

f General Support System (GSS) is interconnected information resources under the same direct management control which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

g Information – means any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

h Information System - means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

i Information Technology (IT) – Refers to computing and/or communication hardware and/or software components and related resources that can collect, store, process, maintain, share transmit or dispose of data. The IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware/software.

j Major Application – An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

k Major Information System – means an information system that requires special management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant role in the administration of agency programs, finances, property or other resources.

l Plan Maintenance – As a general rule, plans should be updated at least semi-annually, when significant change occurs in the IT system or when problem are identified through testing. Contact lists and the emergency call tree should be reviewed and updated frequently.

m Preventive Measures – A risk management process implemented to identify, control and mitigate risk or threats to an IT system in order to reduce or eliminate vulnerabilities and the consequences of threats.

n Recovery Objective – An objective expressed in the delivery of products or services to which an IT system must be recovered in order to meet full business objectives.

o Recovery Time Objective – A time metric derived from the Business Resumption Plan developed by the business owner.

p Risk Management – The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level of risk.

q Roles and Responsibilities – Roles and responsibilities are the functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

r System - A system is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan.

s Teams - Groups comprised of critical IT and business function personnel with various skills, knowledge, and ability to perform necessary functions in order to recover critical IT systems and business functions during a major disruption or event.

t Testing – A mandatory requirement for all plans to validate and evaluate plan procedures and the ability of recovery teams to implement the plan. It identifies any deficiencies in the plan that should be addressed during plan maintenance.