Internal Revenue Service

Unclassified

# Federal Legislative and Regulatory Business Continuity Requirements for the IRS

**Final Version**

Version 1.0

MP 02W0000201

February 28, 2003

Edward S. Talley, CBCP
John J. Reeves

CENTER FOR ENTERPRISE MODERNIZATION
MITRE IRS FFRDC

MITRE

**Center for Enterprise Modernization**
**McLean, Virginia**

# Executive Summary

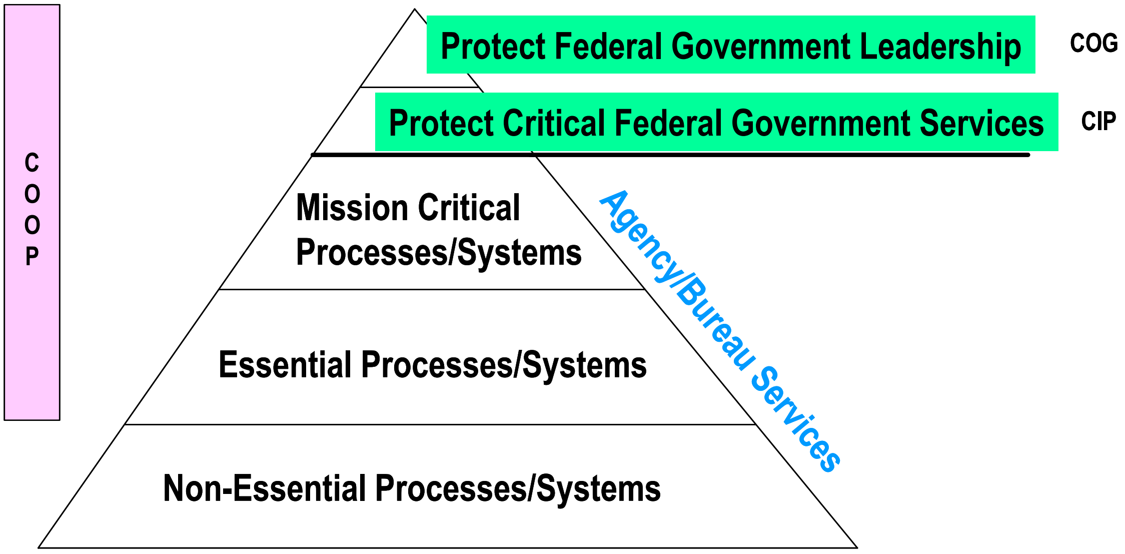
The Internal Revenue Service (IRS), like all federal departments and bureaus, is required to develop an Enterprise Architecture (EA) to illustrate how it fulfills its mission today, and plans to change in the future. Because the subject area of EA is relatively new, there is little guidance available that addresses how a department, agency, or bureau should maintain operations following a major disaster, incident, or disruption. The MITRE Corporation (MITRE) conducted a broad review and analysis of current federal legislation, regulations, and guides to develop this report, which is intended to help the IRS, and other federal agencies, address this need. As part of MITRE's approach, commercial best practices were also investigated. Based on the investigations, MITRE adapted the approach developed by Disaster Recovery Institute, International, with its ten subject areas to categorize applicable business continuity (BC) requirements and the wealth of relevant advice that exists. Although this document was developed for use by the IRS, most of the requirements identified are applicable to all federal civilian agencies. This document is intended for use as a reference source by anyone developing an Enterprise Architecture.

## Continuity of Operations, Critical Infrastructure Protection, and Business Continuity Planning

Every federal agency or bureau is responsible for ensuring its ability to provide any services critical to the maintenance of the U.S. Government. The requirement to maintain critical services is met by planning how to ensure a management structure is available to lead the agency. Management continuity plans are called Continuity of Government (COG) plans. To enable an agency to provide government critical services, certain equipment and facilities are designated as critical and must be specially protected. These assets are called Critical Infrastructure Protection (CIP) assets. COG and CIP plans are concerned with ensuring the continued operation of the U.S. Government.

Every federal agency also determines which processes and systems are mission-critical to them. In the event of a disaster, they must determine which business processes must restored first and which business services can be deferred. They will develop plans for restoring their mission critical services followed by their essential services. They will also make a determination of which services may not be restored until much later.

Continuity of Operations (COOP) plans is a term that encompasses all the plans to restore service: COG, CIP, mission critical, and essential. Business Continuity Planning is the term that covers both the plans and the planning process for all categories of service: COG, CIP, mission critical, essential, and non-essential. Making the decision that something is non-essential is part of Business Continuity Planning. Figure ES–1, Business Continuity Plans Overview, illustrates the relationship between the federal branch requirements and the agency's perspective of its business processes. While all agency mission-critical systems or facilities may not be CIP assets, all CIP assets will be agency mission-critical systems or facilities.


C O O P
Protect Federal Government Leadership
COG
Protect Critical Federal Government Services
CIP
Mission Critical Processes/Systems
Essential Processes/Systems
Non-Essential Processes/Systems
Agency/Bureau Services

• All business processes, systems, and facilities must be considered and prioritized

COOP: Continuity of Operations
COG: Continuity of Government
CIP: Critical Infrastructure Protection

**Figure ES–1. Business Continuity Plans Overview**

## Business Continuity Plans within the IRS

The IRS maintains recovery plans for each Post of Duty. These recovery plans ensure that if a location (facility) became unavailable for an indeterminate period of time, the IRS could quickly assess the impact and execute pre-established plans. The development of these plans required that the IRS determine:

What functions were supported by that facility?

Which organizations were there?

Which of the functions were critical and should be restored quickly?

Who should respond?

- Where should the recovery occur?

Four specific documents capture this information for every IRS facility. The smaller facilities may only have abbreviated versions, but the same questions must be answered for every location. Figure ES–2 shows the specific types of BC plans the IRS uses at its facilities today

- **Plans are developed for each location**
- **The OEP may be executed without executing any other plans**
- **The IMP will identify which BRP and its associated DRP to execute**

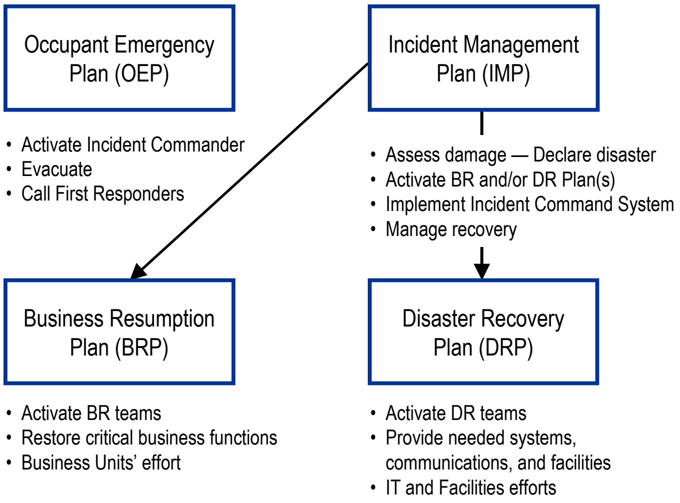

Occupant Emergency Plan (OEP)
Incident Management Plan (IMP)
• Activate Incident Commander
• Evacuate
• Call First Responders
• Assess damage — Declare disaster
• Activate BR and/or DR Plan(s)
• Implement Incident Command System
• Manage recovery
Business Resumption Plan (BRP)
Disaster Recovery Plan (DRP)
• Activate BR teams
• Restore critical business functions
• Business Units' effort
• Activate DR teams
• Provide needed systems, communications, and facilities
• IT and Facilities efforts

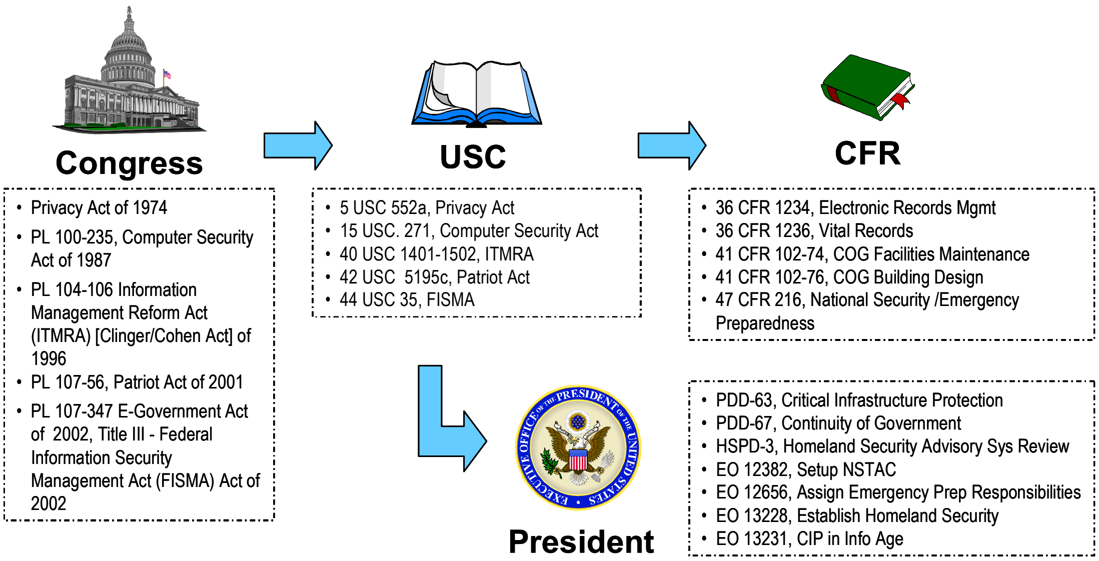
**Figure ES–2. Types of Business Continuity Plans at IRS Facilities**

## Sources of Business Continuity Requirements and Guides

Non-classified documents from federal, Treasury, and IRS sources were reviewed to identify specific documents that have any Business Continuity relevance.

### Sources of Federal Business Continuity Requirements

Most of the requirements identified in this document are derived from the *Congressional Record*, the *Federal Register*, and the National Archives. Current information was gleaned from web sites of independent agencies and offices. Figure ES–3, Sources of Business Continuity Authorizing Documents, shows the applicable laws, U.S. Code (USC), Code of Federal Regulations (CFR), Executive Orders (EO), and Presidential Decision Directives (PDD) that provide directions and authority for some aspect of business continuity. Appendix A contains detailed analysis of each document.



Congress:

- Privacy Act of 1974
- PL 100-235, Computer Security Act of 1987
- PL 104-106 Information Management Reform Act (ITMRA) [Clinger/Cohen Act] of 1996
- PL 107-56, Patriot Act of 2001
- PL 107-347 E-Government Act of 2002, Title III - Federal Information Security Management Act (FISMA) Act of 2002

USC:

- 5 USC 552a, Privacy Act
- 15 USC. 271, Computer Security Act
- 40 USC 1401-1502, ITMRA
- 42 USC 5195c, Patriot Act
- 44 USC 35, FISMA

CFR:

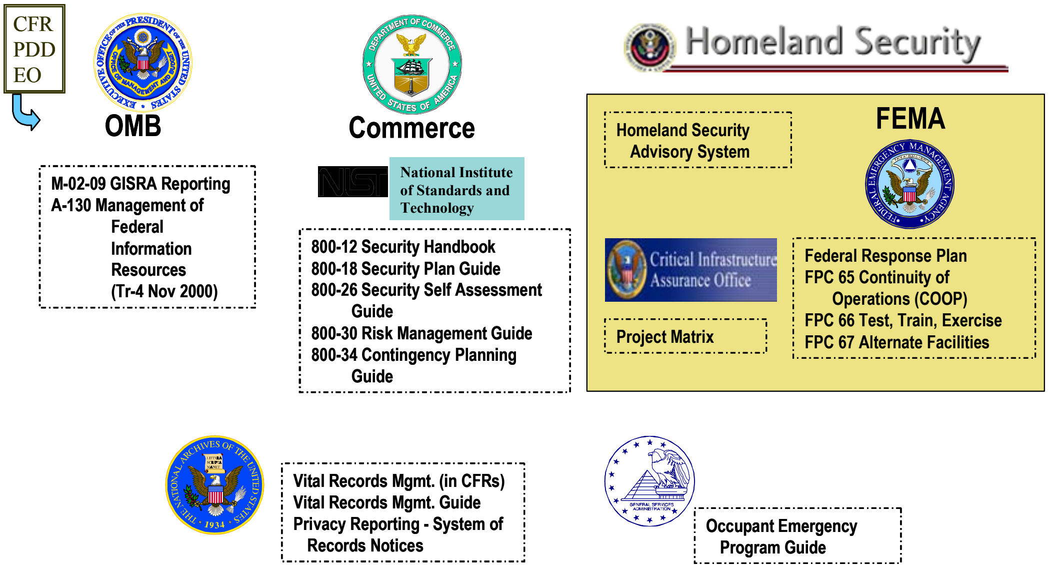
- 36 CFR 1234, Electronic Records Mgmt
- 36 CFR 1236, Vital Records
- 41 CFR 102-74, COG Facilities Maintenance
- 41 CFR 102-76, COG Building Design
- 47 CFR 216, National Security /Emergency Preparedness

President:

- PDD-63, Critical Infrastructure Protection
- PDD-67, Continuity of Government
- HSPD-3, Homeland Security Advisory Sys Review
- EO 12382, Setup NSTAC
- EO 12656, Assign Emergency Prep Responsibilities
- EO 13228, Establish Homeland Security
- EO 13231, CIP in Info Age

**Figure ES–3. Sources of Business Continuity Authorizing Documents**

The documents cited in Figure ES–3 are sources for each department and agency in the Executive Branch to interpret and apply to their specific missions within the federal government. Figure ES–4, Executive Branch Applications of Business Continuity Responsibilities, shows how the responsible departments and agencies have responded with Business Continuity-relevant directives and guides. The appendices contain detailed analyses of each document cited in the figure.


CFR
PDD
EO
OMB
Commerce
National Institute of Standards and Technology
Homeland Security
FEMA
Critical Infrastructure Assurance Office

OMB:

M-02-09 GISRA Reporting
A-130 Management of Federal Information Resources (Tr-4 Nov 2000)

800-12 Security Handbook
800-18 Security Plan Guide
800-26 Security Self Assessment Guide
800-30 Risk Management Guide
800-34 Contingency Planning Guide

Homeland Security:

Homeland Security Advisory System
Project Matrix

FEMA:

Federal Response Plan
FPC 65 Continuity of Operations (COOP)
FPC 66 Test, Train, Exercise
FPC 67 Alternate Facilities

Vital Records Mgmt. (in CFRs)
Vital Records Mgmt. Guide
Privacy Reporting - System of Records Notices

Occupant Emergency Program Guide

**Figure ES–4. Executive Branch Applications of Business Continuity Responsibilities**

Another way of viewing the federal business continuity requirements is by seeing how they have evolved over time. Figure ES 6, the Genealogy of Business Continuity Planning Requirements, illustrates the sequence in which the source documents were developed.

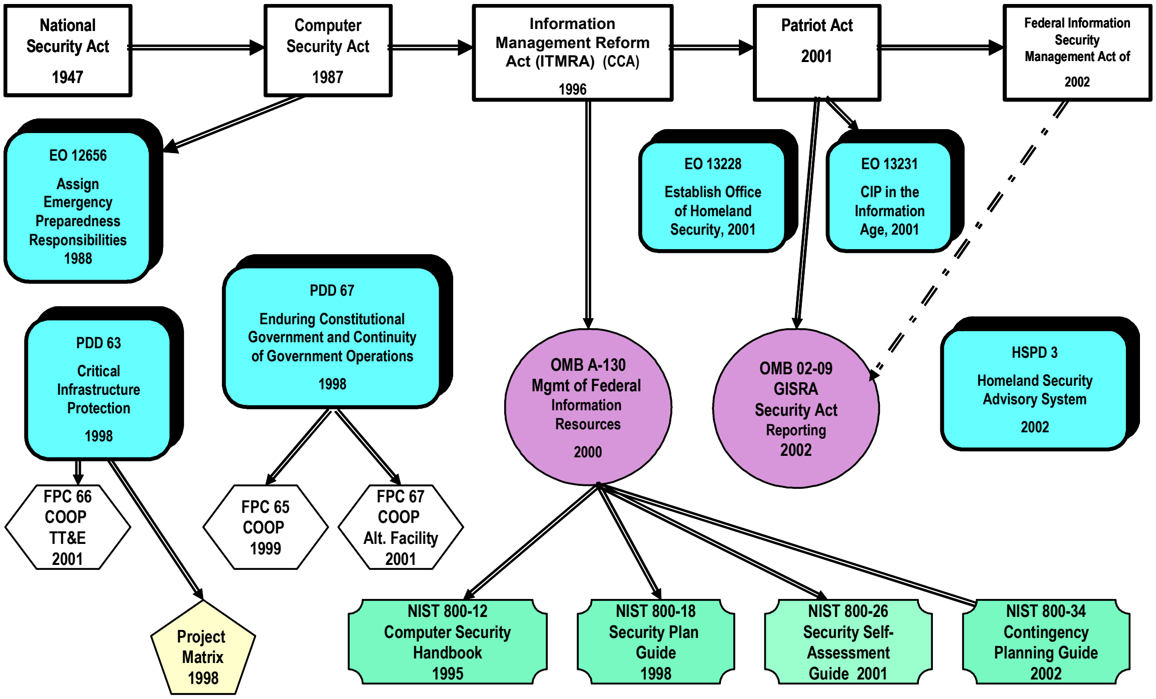
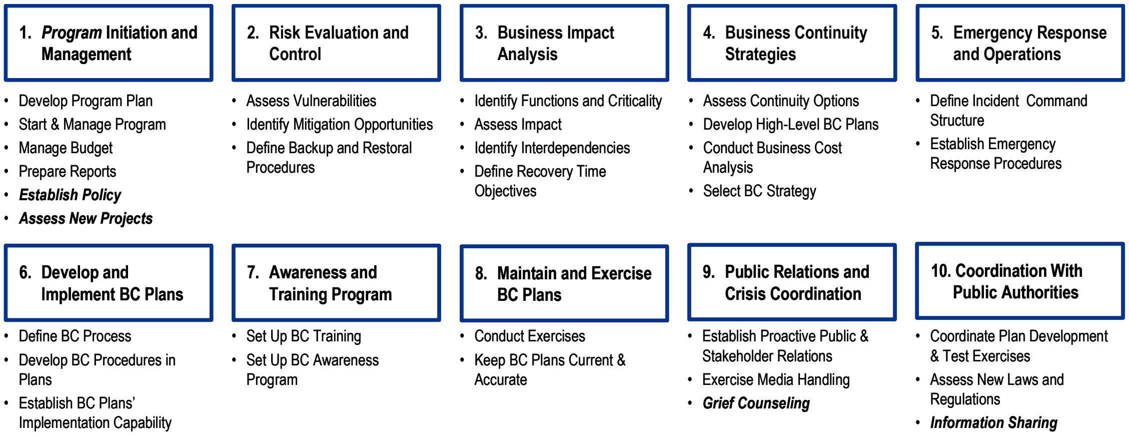

National Security Act 1947
Computer Security Act 1987
Information Management Reform Act (ITMRA) (CCA) 1996
Patriot Act 2001
Federal Information Security Management Act of 2002
EO 12656 Assign Emergency Preparedness Responsibilities 1988
EO 13228 Establish Office of Homeland Security, 2001
EO 13231 CIP in the Information Age, 2001
PDD 67 Enduring Constitutional Government and Continuity of Government Operations 1998
PDD 63 Critical Infrastructure Protection 1998
OMB A-130 Mgmt of Federal Information Resources 2000
OMB 02-09 GISRA Security Act Reporting 2002
HSPD 3 Homeland Security Advisory System 2002
FPC 66 COOP TT&E 2001
FPC 65 COOP 1999
FPC 67 COOP Alt. Facility 2001
Project Matrix 1998
NIST 800-12 Computer Security Handbook 1995
NIST 800-18 Security Plan Guide 1998
NIST 800-26 Security Self-Assessment Guide 2001
NIST 800-34 Contingency Planning Guide 2002

**Figure ES–5. Genealogy of Business Continuity Planning Requirements**

As the basis for the approach and recommendations in this document, MITRE relied on *The Professional Practices for Business Continuity Planners*, the well-recognized industry standard for best practices in the business continuity/disaster recovery industry. *The Professional Practices for Business Continuity Planners* was developed by the Disaster Recovery Institute, International (DRII), which was founded in 1988 to provide a base of common knowledge in contingency planning. DRII also administers the industry's premier global certification program for qualified business continuity and disaster recovery planners. This document is based on the May 2002 version of this business continuity standard.

## Recommended Approach to Address Business Continuity

MITRE recommends using the DRI model with a few additions, as noted in italics in Figure ES–6, to address the specific concerns of the federal government that are not present in the commercial model. The DRI model provides a suitable framework for associating existing federal requirements and advisories to common BC subject areas. The appendices contain the detailed results of MITRE’s analysis of the requirements. Each requirement or advisory and source is collected under the applicable subject area(s). The complete list provides the business continuity requirements that the IRS and other federal agencies should address.



**1. *Program* Initiation and Management**

- Develop Program Plan
- Start & Manage Program
- Manage Budget
- Prepare Reports
- ***Establish Policy***
- ***Assess New Projects***

**2. Risk Evaluation and Control**

- Assess Vulnerabilities
- Identify Mitigation Opportunities
- Define Backup and Restoral Procedures

**3. Business Impact Analysis**

- Identify Functions and Criticality
- Assess Impact
- Identify Interdependencies
- Define Recovery Time Objectives

**4. Business Continuity Strategies**

- Assess Continuity Options
- Develop High-Level BC Plans
- Conduct Business Cost Analysis
- Select BC Strategy

**5. Emergency Response and Operations**

- Define Incident Command Structure
- Establish Emergency Response Procedures

**6. Develop and Implement BC Plans**

- Define BC Process
- Develop BC Procedures in Plans
- Establish BC Plans' Implementation Capability

**7. Awareness and Training Program**

- Set Up BC Training
- Set Up BC Awareness Program

**8. Maintain and Exercise BC Plans**

- Conduct Exercises
- Keep BC Plans Current & Accurate

**9. Public Relations and Crisis Coordination**

- Establish Proactive Public & Stakeholder Relations
- Exercise Media Handling
- ***Grief Counseling***

**10. Coordination With Public Authorities**

- Coordinate Plan Development & Test Exercises
- Assess New Laws and Regulations
- ***Information Sharing***

Source: *Professional Practices for Business Continuity Planners*, *Modified,* DRI International, May 2002

Note: *Italics* represent proposed changes to the DRI model to include Federal Government needs.

**Figure ES–6. Federal Government Approach to Managing Business Continuity**

It is intended that the composite list of requirements in Section 6 will be used to conduct a business continuity "as is" review of the Enterprise Architecture to determine the level of compliance within the agency.

## Sample of Business Continuity Requirements

Table ES–1 presents a sample of the business continuity requirements applicable to the first subject area in the DRI model, Program Initiation and Management. This sample illustrates only one reference from each of the sources that contain references. As noted, the appendices contain detailed analyses of each source document. The number in parentheses indicates the specific numbered entry in the analysis table within the applicable appendices that applies to this source.

**Table ES–1. Sample Requirement Descriptions: Program Initiation and Management**

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 1. | Computer systems require Security Plans | Computer Security Act (3) |
| 2. | Establish a plan for the security and privacy of each Federal computer system | Computer Security Act (6) |
| 3. | Ensure that the information security policies, procedures, and practices are adequate | Clinger/Cohen (10) |
| 4. | Minimize Critical Infrastructure disruptions | Patriot Act (2) |
| 5. | Federal agency responsibilities<br>The head of each agency shall be responsible for providing information security protections | FISMA (2) |
| 6. | Each agency shall develop, document, and implement an agency wide information security program …, that includes:<br>…(2) policies and procedures | FISMA (4) |

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 7. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. | FISMA (9) |
| 8. | Agencies shall conduct a vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure. | PDD-63 (10) |
| 9. | Homeland Security Advisory System shall be binding on the executive branch | HSPD-3 (2) |
| 10. | HSPD Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. | HSPD-3 (3) |
| 11. | The CIP program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. | EO 13231 (2) |
| 12. | Agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately addresses these mission areas. | EO 13231 (6) |
| 13. | Coordinate [Recruitment, Retention, and Training] programs to ensure that government employees with responsibilities for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, are adequately trained and evaluated | EO 13231 (12) |
| 14. | Heads of agencies are responsible for the vital records program. | 36CFR1236 (3) |
| 15. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 16. | Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities. | NIST SP 800-12 (8) |
| 17. | Contingency plans must be based on a clearly defined policy | NIST SP 800-34 (4) |

## Number of References Identified for Each Subject Area

MITRE's research was organized in the DRII 10 subject areas. Table ES–2 summarizes the number of BC requirements and advice references for each subject area that were identified in this effort.

**Table ES–2. Summary of Identified Business Continuity Requirements and References**

| Area # | Subject Area | Total Requirements Identified | Total Advice References Identified |
|---|---|---|---|
| 1 | Project Initiation & Management | 44 | 18 |
| 2 | Risk Evaluation & Control | 34 | 18 |
| 3 | Business Impact Analysis | 42 | 8 |
| 4 | Business Continuity Strategies | 51 | 19 |
| 5 | Emergency Response & Operations | 36 | 17 |
| 6 | Develop & Implement BC Plans | 61 | 14 |
| 7 | Awareness & Training Program | 25 | 4 |
| 8 | Maintain & Exercise BC Plans | 57 | 7 |
| 9 | Public Relations and Crisis Coordination | 15 | 22 |
| 10 | Coordination with Public Authorities | 11 | 9 |
| | **Total** | 376 | 136 |

## Conclusion

Even though the term "business continuity" is only just starting to be adopted, there is overwhelming evidence that all federal departments and agency/bureaus have many existing sources of requirements that must be considered when developing an Enterprise Architecture. This report identifies most, if not all, of those sources for business continuity requirements. In addition, it is apparent that every federal agency should establish an ongoing program to develop and maintain a business continuity capability.

# Table of Contents

# List of Figures

# List of Tables

# 1. Introduction

The Internal Revenue Service (IRS), like all federal departments and bureaus, is required to develop an Enterprise Architecture (EA) to illustrate how it fulfills its mission today, and plans to change in the future. Because the area of EA is relatively new, there is little guidance available that addresses how a department, agency, or bureau should maintain operations following a major disaster, incident, or disruption. This report by The MITRE Corporation (MITRE) looks at the federal regulations and guides for direction on how to address Business Continuity (BC) concerns within the IRS, or any federal agency. MITRE has applied an approach for organizing the requirements that follows current industry trends. This report is intended to identify all current and applicable requirements for business continuity that would be used to conduct an "as is" analysis of the Enterprise Architecture.

## 1.2. Purpose

This report identifies federal laws and regulations, Department of the Treasury (Treasury) directives, IRS Manual requirements, and guidance applicable to business continuity that federal agencies and the IRS in particular, need to address. This report is intended to be used as a reference source by anyone developing an Enterprise Architecture.

## 1.3. Background

The concept of business continuity has been evolving from the simple advice—"backup your data"—to a mission objective—"maintain 24 x 7 operations." In this evolution, different parts of the organization have played somewhat independent roles. The Information Technology (IT) area has assumed responsibility for maintaining the computing capability. The Security Department has been concerned with protecting the computers and the data. The Business Areas have been concerned with providing continued service. Business Continuity combines aspects of all three areas in an integrated set of plans and procedures that will ensure that the organization can quickly recover from any type of major disruption.

Both the commercial world and the federal government have been following the same path toward an enterprise approach to plan and manage business continuity. This report also addresses the evolution of those efforts.

## 1.4. Scope of This Document

Although this report was developed for the Internal Revenue Service, it is applicable to all federal civilian departments, agencies, and bureaus. The intent was to review all current federal laws, directives, and guides that do not have a National Security classification. Because many of the auditor's reports are classified as Limited Official Use (LOU), this report only represents the generic intent.

## 1.5. Methodology

This report was developed by reviewing publicly available information through Government-owned web sites. In addition, both the Treasury Critical Infrastructure Protection Plan, Version 2 (TCIPP) and IRS Manual's Security section were analyzed, and this report includes generic requirements from those documents. No classified or sensitive information is contained in this report.

The List of References identifies the documents that were assessed or researched by MITRE. Where applicable, each citation indicates whether or not relevant business continuity requirements were found in the reference document. The goal was to determine which document superceded others; the analysis presented involves only the latest version still in effect. For each reference that contained applicable business continuity requirements, a separate analysis table was created that captured the text of the requirement. The appendices contain the applicable quotes from the reference sources. Each appendix table captures business continuity requirements and advice necessary for a current assessment of any federal Enterprise Architecture for its business continuity support capability.

## 1.6. Document Organization

| Section | | Purpose |
|---|---|---|
| Section 1: | Introduction | Describes the purpose and use of this document |
| Section 2: | Understanding Business Continuity Management | Discusses terminology and concepts |
| Section 3: | Where the Requirements Come From | Discusses roles and products of Federal Executive Branch applicable to Business Continuity |
| Section 4: | Current Business and Government BC Best Practices | Describes current state of the art in Business Continuity |
| Section 5: | Recommended Approach to Address Business Continuity | Describes ten subject areas that need to be defined to completely address Business Continuity |
| Section 6: | Business Continuity Functional Requirements | Associates specific requirements identified in the references to ten subject areas |
| Appendix A: | Federal Requirements and Guides | Detailed identification of specific references that contain requirements for Business Continuity |
| Appendix B: | Treasury Requirements | Detailed analysis of current Treasury documents that have specific Business Continuity relevance |
| Appendix C: | IRS Requirements | Detailed analysis of current Internal Revenue Service documents that have specific Business Continuity relevance |
| Appendix D: | Auditor's Recommendations | Generic analysis of GAO and TIGTA recommendations that relate to Business Continuity Management |

| Section | Purpose |
|---|---|
| Acronym List | Provides a list of acronyms used throughout the document |
| Glossary | Provides some definition of Business Continuity terms |
| List of References | Provides a complete list of all documents reviewed for this report (and includes those references determined to not have Business Continuity relevance) |

# 2. Understanding Business Continuity Management

Business Continuity Management (BCM) is the term currently used to describe the roles and responsibilities an organization should adopt and use to ensure its ability to quickly recover from any major disruption of service at any of its locations. BCM encompasses management, budgeting, planning, training, maintaining, and execution of plans.

## 2.1 Evolution of Information Technology Security to Business Continuity

Looking back at the history of computing provides an understanding of how Business Continuity has evolved. At first, as shown in Figure 1, Evolution of Business Continuity*,* the concern was to save the data with a backup to a floppy disk; as the data volume increased, magnetic tape was used. Later, it was recognized that information should also be stored off site. Ultimately, concerns were raised that, in addition to protecting the data, the processing power also should be duplicated to ensure an ability to quickly restore IT services. While that activity was occurring, it became apparent that problems could occur if the information were misused, inspiring the idea to protect it.

Thus, the cyber security area emerged to protect the data and processing powers. Initially, security plans addressed how to employ passwords to prevent the unauthorized use of applications. Next, security professionals recognized the need to protect the system that ran the applications. Finally, Computer Emergency Response teams were set up to protect the facility from unauthorized access. The Security Division has been responsible for IRS facilities, and quickly adapted to the need to protect the organization's cyber assets as well. The efforts of the IT Division and Security Division resulted in contingency plans to protect the IRS computer systems and ensure their restorable, if the need arose.

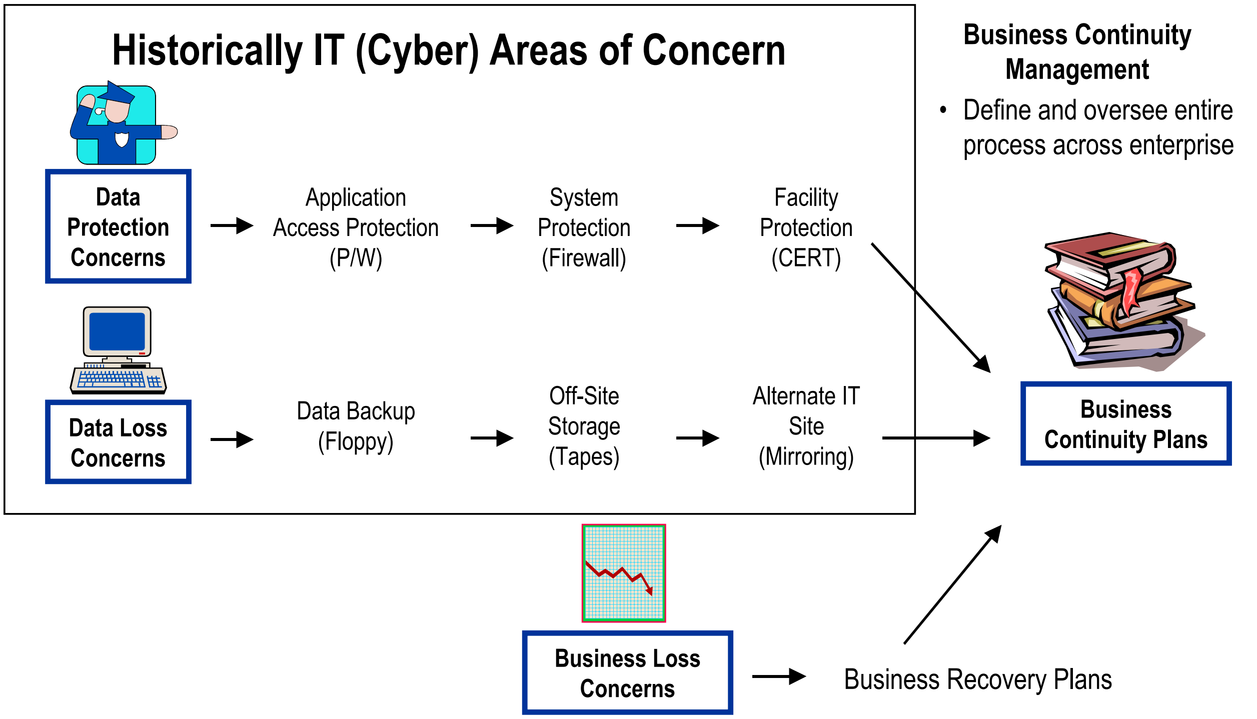

Historically IT (Cyber) Areas of Concern
Business Continuity Management
• Define and oversee entire process across enterprise
Data Protection Concerns
Application Access Protection (P/W)
System Protection (Firewall)
Facility Protection (CERT)
Data Loss Concerns
Data Backup (Floppy)
Off-Site Storage (Tapes)
Alternate IT Site (Mirroring)
Business Continuity Plans
Business Loss Concerns
Business Recovery Plans

**Figure 1. Evolution of Business Continuity**

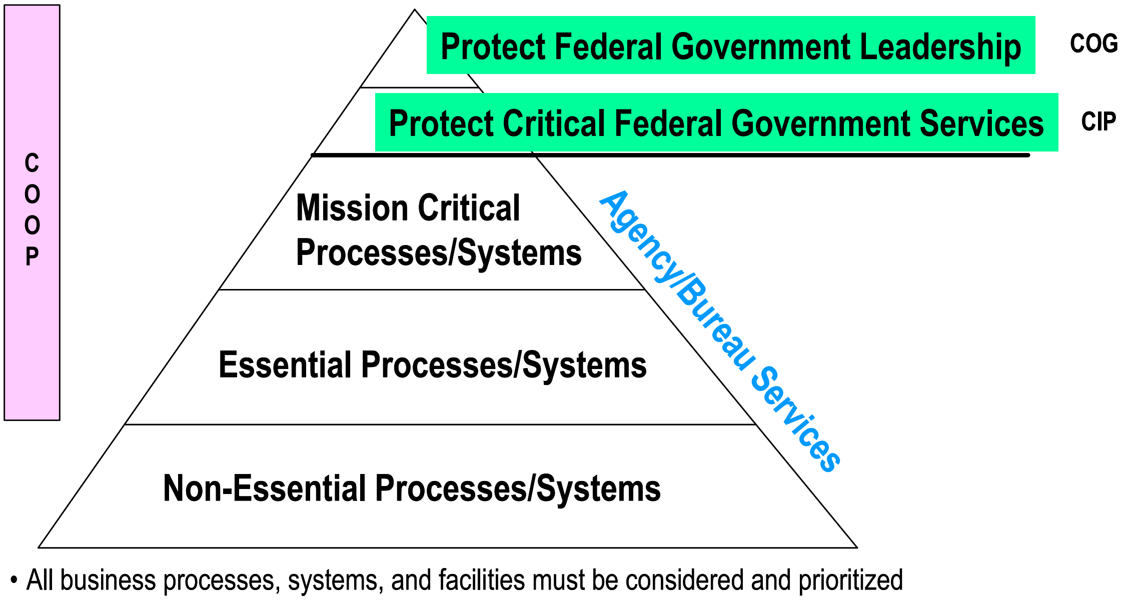
As this was occurring, the business users became concerned that even if the IT department could reconstitute service at another facility, the mission was nevertheless threatened unless there was good planning to get people to the new facility. The business users developed their own business recovery plans, which were often unconnected to or, worse yet, even controlled the IT contingency plans. Thus, it became necessary to develop business continuity management that tied the IT and business users' plans and capabilities together to ensure continuity of mission-critical services following any major service interruption.

## 2.2 Continuity of Operations, Critical Infrastructure Protection, and Business Continuity Planning

Every federal agency or bureau is responsible for ensuring its ability to provide any services critical to the maintenance of the U.S. Government. The requirement to maintain critical services is met by planning how to ensure a management structure is available to lead the agency. Management continuity plans are called Continuity of Government (COG) plans. To enable an agency to provide government critical services, certain equipment and facilities are designated as critical and must be specially protected. These assets are called Critical Infrastructure Protection (CIP) assets. COG and CIP plans are concerned with ensuring the continued operation of the U.S. Government.

Every federal agency also determines which processes and systems are mission-critical to them. In the event of a disaster, they must determine which business processes must restored first and which business services can be deferred. They will develop plans for restoring their mission critical services followed by their essential services. They will also make a determination of which services may not be restored until much later.

Continuity of Operations (COOP) plans is a term that encompasses all the plans to restore service: COG, CIP, mission critical, and essential. Business Continuity Planning is the term that covers both the plans and the planning process for all categories of service: COG, CIP, mission critical, essential, and non-essential. Making the decision that something is non-essential is part of Business Continuity Planning. Figure 2 Business Continuity Plans Overview, illustrates the relationship between the federal branch requirements and the agency's perspective of its business processes. While all agency mission-critical systems or facilities may not be CIP assets, all CIP assets will be agency mission-critical systems or facilities.


C O O P
Protect Federal Government Leadership
COG
Protect Critical Federal Government Services
CIP
Mission Critical Processes/Systems
Essential Processes/Systems
Non-Essential Processes/Systems
Agency/Bureau Services
• All business processes, systems, and facilities must be considered and prioritized

| | |
|---|---|
| COOP: | Continuity of Operations |
| COG: | Continuity of Government |
| CIP: | Critical Infrastructure Protection |

**Figure 2. Business Continuity Plans Overview**

## 2.3 Business Continuity Plans within the IRS

The IRS maintains recovery plans for each Post of Duty. These recovery plans ensure that if a location (facility) becomes unavailable for an indeterminate period of time, the IRS could quickly assess the impact and execute pre-established plans. The development of these plans required that the IRS determine:

- What functions were supported by that facility?
- Which organizations were there?
- Which functions were critical and should be restored quickly?
- Who should respond?
- Where should the recovery occur?

Four specific documents capture this information for every IRS facility. The smaller facilities may only have abbreviated versions, but the same questions must be answered for every location. Figure 3, Types of Business Continuity Plans at a Facility, illustrates the specific types of business continuity plans the IRS uses at its facilities today.

- **Plans are developed for each location**
- **The OEP may be executed without executing any other plans**
- **The IMP will identify which BRP and its associated DRP to execute**

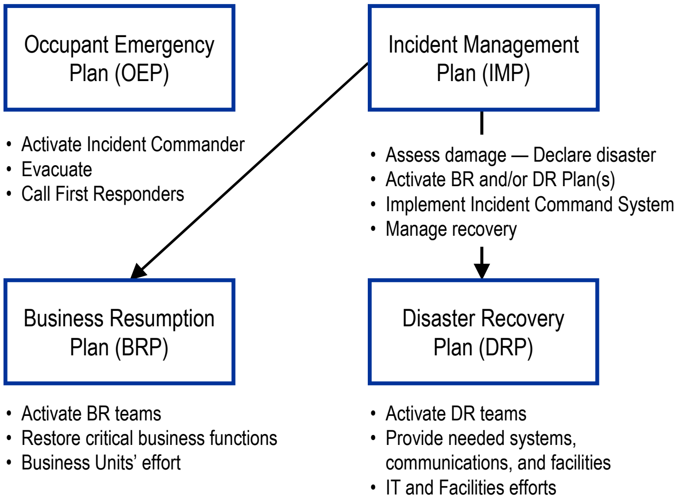

Occupant Emergency Plan (OEP)
• Activate Incident Commander
• Evacuate
• Call First Responders
Incident Management Plan (IMP)
• Assess damage — Declare disaster
• Activate BR and/or DR Plan(s)
• Implement Incident Command System
• Manage recovery
Business Resumption Plan (BRP)
• Activate BR teams
• Restore critical business functions
• Business Units' effort
Disaster Recovery Plan (DRP)
• Activate DR teams
• Provide needed systems, communications, and facilities
• IT and Facilities efforts

**Figure 3. Types of Business Continuity Plans at a Facility**

### 2.3.1 Business Continuity Management Plan

Within the context of this report, the term Business Continuity Management Plan will be used to identify any and all policies, procedures, cost studies, business impact analyses, risk assessments, business continuity strategies, testing methodologies and plans, training plans, and organizational descriptions that discuss how the enterprise will manage its business continuity efforts.

### 2.3.2 Occupancy Emergency Plan

**What is an Occupancy Emergency Plan (OEP)**?[1]

The Federal Management Regulations (FMR) specifically requires the General Services Administration (GSA) to assist federal agencies that occupy federally owned or leased facilities in establishing and maintaining an Occupant Emergency Program (OEP).

The FMR defines an OEP as "… a short-term emergency response program [that] establishes procedures for safeguarding lives and property during emergencies in particular facilities."

**What is an occupant emergency?**

An occupant emergency is an event that requires personnel to be evacuated from occupied space or relocated to a safer area. The emergency may be a fire, explosion, discovery of an explosive device, severe weather, earthquakes, chemical or biological exposure or threat, hostage takeover or physical threat to building occupants or visitors.

[1] General Services Administration Public Building Service, Federal Protective Service – Occupant Emergency Program Guide, March 2002

**What preparations do I need to take?**
You need to have established these three things:

- Occupancy Emergency Plan Designated Official
- Occupancy Emergency Program
- Occupancy Emergency Organization

**Who is the Designated Official (DO)?**
The Designated Official is the highest-ranking official in a federal facility or another person agreed on by all tenant agencies. In the absence of the DO, an alternate official(s) may be designated to carry out the duties.

**Who represents the DO after normal duty hours?**
The senior federal official present represents the DO or alternate and handles emergencies according to the plan.

**What is an Occupancy Emergency Program?**
It's a program establishing procedures for safeguarding lives and property in and around the facility during emergencies.

### 2.3.3 Incident Management Plan

The concepts in the Incident Management Plan are based upon on the industry's Standard Emergency Management System (SEMS) structure used for incident management.[2] The Senior Commissioner's Representative or the Commissioner's Representative (SCR/CR) serves as the IRS Emergency Management Official and has the responsibility for managing the crisis response and the subsequent recovery of site operations. The SCR/CR, or designated alternate for smaller Posts of Duty (POD), will assume the role of the IRS Incident Manager (IM) and interface, as needed, with Incident Managers/Commanders at other agencies or emergency services during the incident.

The IM will establish command and manage the incident utilizing personnel and resources located at the site irrespective of the site personnel's normal reporting relationship or assignment. The IM will manage all response and recovery activities with assistance from designated personnel of Business Units and Information Technology systems on the recovery team. Business Units and Information Technology (ITS)/Agency Wide Shared Services (AWSS) staff will utilize their applicable Business Resumption (BR) and Disaster Recovery (DR) Plans as directed by the Incident Manager. The IM will ensure that the business processes critical to the IRS are recovered in a priority order consistent with Critical Business Priorities list developed for the facility.

[2] IRS Post of Duty Business Continuity Incident Management Plan, Draft February 28, 2002

The IRS Incident Command Management Structure involves:

- **Incident Management Team** – Provides the overall direction and sets priorities during the emergency;
- **Operations Team** – Implements priorities established by management through sub teams;
- **Planning Team** – Gathers and assesses information and documents emergency activities;
- **Logistics Team** – Obtains the resources to support the emergency operations; and
- **Finance/Administration Team –** Manages all costs relating to the emergency operations.

If the facility experiencing the incident does not have sufficient staff or expertise to assign to the recovery teams, the Incident Manager must solicit help from other facilities or service providers.

During any emergency situation the Incident Management Team (IMT) will report to the Crisis Management Center (CMC) designated in the Occupancy Emergency Plan and identified in the Location Description form. The IMT will work out of the CMC unless another location is designated.

### 2.3.4 Business Resumption Plan

The Business Resumption Plan (BRP) documents the recovery strategies, personnel, procedures, and resources that the Business Resumption Work Group will use to respond to any short- or long-term interruption to its essential business functions.[3] A Business Operating Division (BOD) or Functional Operating Division (FOD) may include several business functions/processes at a site. There is a BRP for each BOD and FOD located at the facility.

The BRP is organized so that one need not read every word in order to determine the appropriate actions and activities necessary to recover. The BRP is a combination disaster time checklist, reference document, and training aid. Each part of the BRP should be assessed based on the incident circumstances to determine whether it should be activated.

The BRP has the following limitations:

1. The scope of the BRP is limited to any incident that can occur at the IRS location identified in the Location Description and in the header of this document.
2. The BRP only provides high-level procedures and essential information and checklists during the incident.
3. Most information in the BRP must be provided **before** the incident.

[3] IRS Post of Duty– Business Continuity Business Resumption Plan (BRP), Draft March 4, 2002

### 2.3.5 Disaster Recovery Plan

This Disaster Recovery Plan (DRP) documents the systems, telecommunication requirements, strategies, personnel, procedures, and resources that the IT and Telecommunications Recovery Teams will use to respond to any short- or long-term interruption to IT and telecommunications services to the site and to the site's essential business functions. The DRP and its use are the responsibility of the servicing ITS organization for the site.

The DRP identifies the teams for the recovery of IT systems and telecommunication systems at the site. These teams are responsible for meeting the IT and telecommunications needs of the business functions being recovered at an alternate site, identified in the BRP for that function or work group. Recovery of the IT systems will be managed by the IT Recovery Team. Recovery of the telecommunications systems will be managed by the Telecommunications Recovery Team. These teams may be activated following detection of an incident or at the direction of the Incident Management Team or DRP Recovery Team Leaders.

The Incident Manager may activate the DRP at any time during the emergency evaluation process by notifying the Disaster Recovery Manager of an incident requiring activation of the plan.

The DRP has the following limitations:

1. The scope of the DRP is limited to the management of any incident that can occur at the IRS location identified in the facility named on the cover.

2. The DRP only provides essential information needed by a DR Manager to use during the incident. Procedures to be followed by various members of the DR Team will be identified as part of the development of this DRP.

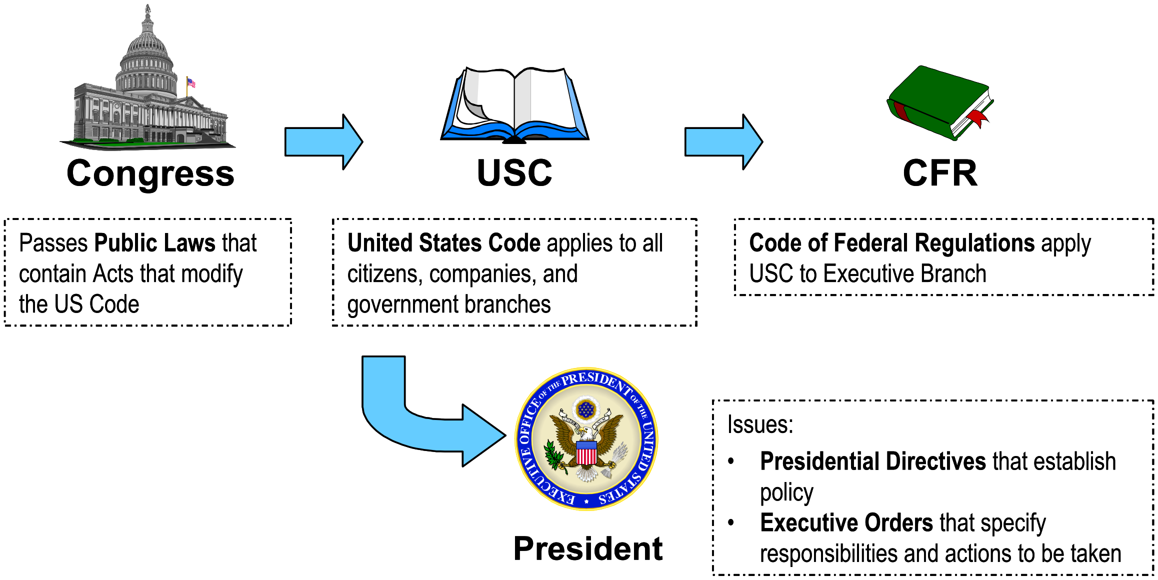
3. Most information in the DRP must be provided **before** the incident.

# 3. Where the Requirements Come From

The sources of requirements that every federal agency is required to follow were reviewed to determine the requirements for Business Continuity Planning and Management. The relationships between these sources and their authorities are not often clear. This section identifies the generic sources of requirements or guides for any federal Executive Branch agency and the types of business continuity information they provide.

## 3.1 Generic Flow Department and Bureau/Agency Requirements

All department and bureau/agency requirements originate with Public Laws passed by Congress and approved by the President of the United States. As shown in Figure 4, the Public Laws contain Acts that specify how the USC is to be modified. The USC codifies the roles, responsibilities, and authorities for the Executive Branch. The President is responsible for directing the Executive Branch in implementing the USC. While the USC describes the high-level requirements for departments and agencies, the Code of Federal Regulations provides detailed operating requirements for each individual organization within the Executive Branch. The USC authorizes the President to establish policy and direct the Executive Branch. Policy decisions by the President are contained in Presidential Decision Directives. Specific directions to each department or agency are provided in Executive Orders.



Passes **Public Laws** that contain Acts that modify the US Code

**United States Code** applies to all citizens, companies, and government branches

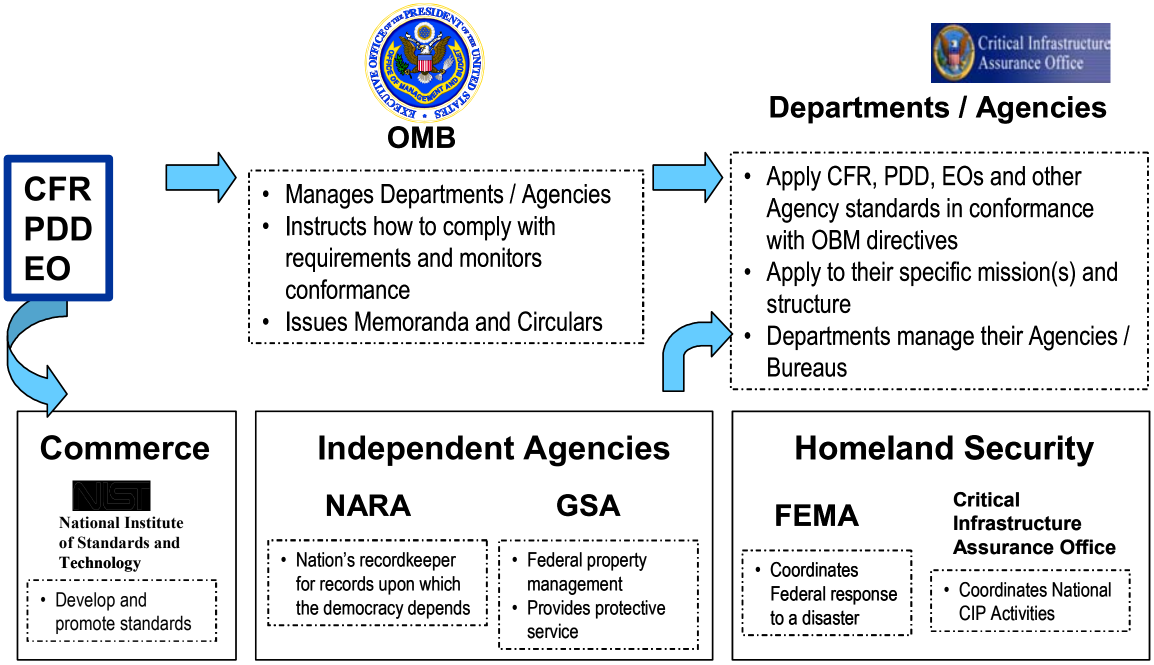
**Code of Federal Regulations** apply USC to Executive Branch

Issues:

- **Presidential Directives** that establish policy
- **Executive Orders** that specify responsibilities and actions to be taken

**Figure 4. Requirements Flow from Public Laws to Presidential Decisions**

The Office of Management and Budget (OMB) is responsible for directing all federal departments and agencies. OMB provides requirements for consistent reporting and budgeting across all departments and agencies. Figure 5, Requirements Flow to Departments and Agencies, depicts generically how requirements flow from PDDs, EOs, and the CFR.



CFR
PDD
EO

OMB

- Manages Departments / Agencies
- Instructs how to comply with requirements and monitors conformance
- Issues Memoranda and Circulars

Departments / Agencies

- Apply CFR, PDD, EOs and other Agency standards in conformance with OBM directives
- Apply to their specific mission(s) and structure
- Departments manage their Agencies / Bureaus

Commerce

National Institute of Standards and Technology

- Develop and promote standards

Independent Agencies

NARA

- Nation's recordkeeper for records upon which the democracy depends

GSA

- Federal property management
- Provides protective service

Homeland Security

FEMA

- Coordinates Federal response to a disaster

Critical Infrastructure Assurance Office

- Coordinates National CIP Activities

**Figure 5. Requirements Flow to Departments and Agencies**

In the area of Business Continuity, the National Institute of Standards and Technology (NIST within the Department of Commerce, National Archives and Records Administration (NARA), General Services Administration (GSA), and within the new Department of Homeland Security, the Federal Emergency Management Agency (FEMA) and Critical Infrastructure Assurance Office CIAO) all have specific roles, responsibilities, and authorities. The National Institute of Standards and Technology (NIST), is responsible for developing and promoting standards throughout the federal government. The Critical Infrastructure Assurance Office (CIAO), has responsibility for coordinating all federal efforts to maintain all systems, processes, and facilities critical to the maintenance of the U.S. Government. National Archives and Records Administration (NARA) establishes standards for maintain information. The General Services Administration establishes rules and procedures for evacuating buildings that they lease.

### 3.1.1 Office of Management and Budget

The Office of Management and Budget's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures; assesses competing funding demands among agencies; and sets funding priorities. OMB ensures that all agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies.

In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public.

OMB issues Circulars to disseminate information, to establish policies and procedures, or to issue instructions. OMB also issues Memoranda to direct specific actions to be taken by "Heads of Executive Departments and Agencies."

### 3.1.2 National Institute of Standards and Technology

Founded in 1901, the National Institute of Standards and Technology is a non-regulatory federal agency within the Department of Commerce's Technology Administration. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

NIST's Computer Security Division (CSD) is one of eight divisions within the NIST Information Technology Laboratory. The mission of the CSD is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems
- Developing standards, metrics, tests, and validation programs to

  Promote, measure, and validate security in systems and services
  Educate consumers
  Establish minimum security requirements for federal systems
- Developing guidance to increase secure IT planning, implementation, management, and operation.

NIST publishes guides in the form of Special Publications that identify standardized terminology and methodologies to be used throughout the federal government.

Federal organizations may be particularly interested in monitoring NIST security programs and services. These are grouped by (1) security policies, standards, and guidelines; (2) security validated products; (3) training and education; and (4) collaborative work and services.

### 3.1.3 Critical Infrastructure Assurance Office

The Critical Infrastructure Assurance Office was created in May 1998 by PDD-63, which also designated a lead agency for each of the major sectors of our economy that are vulnerable to infrastructure attack. In January 2003, the National CIAO was transferred under the Department of Homeland Security.

The CIAO's responsibilities for developing and coordinating national critical infrastructure assurance policy focus primarily on three key areas:

- Promoting national outreach and awareness campaigns, both in the private sector and at the state and local government level

- Assisting federal agencies to analyze their own risk exposure and critical infrastructure dependencies
- Coordinating the preparation of an integrated national strategy for critical infrastructure assurance.

Critical Infrastructures comprise those industries, institutions, networks, and systems essential to the nation's defense and economic security, and to the health, welfare, and safety of its citizens.

These infrastructures relate to:

- Information and communications
- Electric power generation, transmission, and distribution
- Oil and gas production and distribution
- Banking and finance
- Transportation
- Water supply
- Emergency government services.

Critical infrastructure assurance is concerned with the readiness, reliability, and continuity of services. Critical infrastructure assurance is designed to reduce the vulnerability to disruptions, shorten the duration of any impairment and limit its scale, and readily restore services when disruptions occur.

### 3.1.4 National Archives and Records Administration

The National Archives and Records Administration (NARA), an independent federal agency, is America's national record keeper. NARA's mission is to ensure ready access to the essential evidence that documents the rights of American citizens, the actions of federal officials, and the national experience.

NARA is a public trust upon which our democracy depends. NARA enables people to inspect for themselves the record of what government has done. NARA enables officials and agencies to review their actions and helps citizens hold them accountable for those actions.

To be effective, NARA must do the following:

- Determine what evidence is essential for such documentation and ensure that the government creates such evidence
- Make it easy for users to access that evidence regardless of where it is, where they are, and for as long as needed

- Find technologies, techniques, and partners worldwide that can help improve service and hold down cost
- Help staff members continuously expand their capability to make the changes necessary to realize the vision.

NARA defines requirements for handling vital records and reporting of privacy record management in the Federal Register.

### 3.1.5 General Services Administration

The General Services Administration is a centralized federal procurement and property management agency created by Congress to improve government efficiency and effectiveness. The Federal Property and Administrative Services Act of 1949 consolidated the procurement and property management activities of several agencies into one “to provide for the Government an economical and efficient system” for the procurement, supply, and disposal of real property, personal property and services, as well as “uniform policies and methods of procurement, supply and related functions.”

GSA’s mission is to help federal agencies better serve the public by offering, at best value, superior workplaces, expert solutions, acquisition services and management policies.

Through its Federal Protective Service, GSA is responsible for the safety and security of federal government tenants and visitors to GSA space. This responsibility has evolved from a reactive posture of patrol and incident response to a proactive stance of crime prevention and threat reduction. In the aftermath of September 11, 2001, GSA has redoubled its efforts to provide a safe and secure environment. In addition to the enhanced security levels, GSA is reaching out to tenants, updating occupant emergency plans, conducting classes on crime prevention and anthrax, and doing mailroom searches for hazardous materials.

### 3.1.6 Federal Emergency Management Administrations

The Federal Emergency Management Administration (FEMA) was an independent federal agency with more than 2,600 full-time employees until it was transferred under the Department of Homeland Security in January 2003. FEMA’s main offices are in Washington D.C., at regional and area offices across the country, at the Mount Weather Emergency Operations Center, and at the FEMA training center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available to help out after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies, and the American Red Cross.

FEMA is responsible for advising on building codes and flood plain management; teaching people how to get through a disaster; helping equip local and state emergency preparedness; coordinating the federal response to a disaster; making disaster assistance available to states, communities, businesses, and individuals; training emergency managers; supporting the nation’s fire service; and administering the national flood and crime insurance programs.

One way to look at what FEMA does is to think about the life cycle of disasters. The disaster life cycle describes the process through which emergency managers prepare for emergencies and disasters, respond to them when they occur, help people and institutions recover from them, mitigate their effects, reduce the risk of loss, and prevent disasters such as fires from occurring. And at every stage of this cycle one sees FEMA—the federal agency charged with building and supporting the nation's emergency management system.

## 3.2 Sources of Business Continuity Requirements and Guides

Non-classified documents from federal, Treasury, and IRS sources were reviewed to identify the specific documents that have any Business Continuity relevance.

## 3.3 Federal Business Continuity Requirements Sources

The Congressional Record, the Federal Register, and the National Archives served as the sources for most of the references used in this report. Additionally, web sites from independent agencies and offices provided current information. Figure 6 illustrates the results of MITRE's search, showing the applicable laws, USC sections, CFR sections, Executive Orders, and Presidential Decision Directives that provide directions and authority for some aspect of business continuity. Appendix contains detailed analysis of each document cited in this figure.

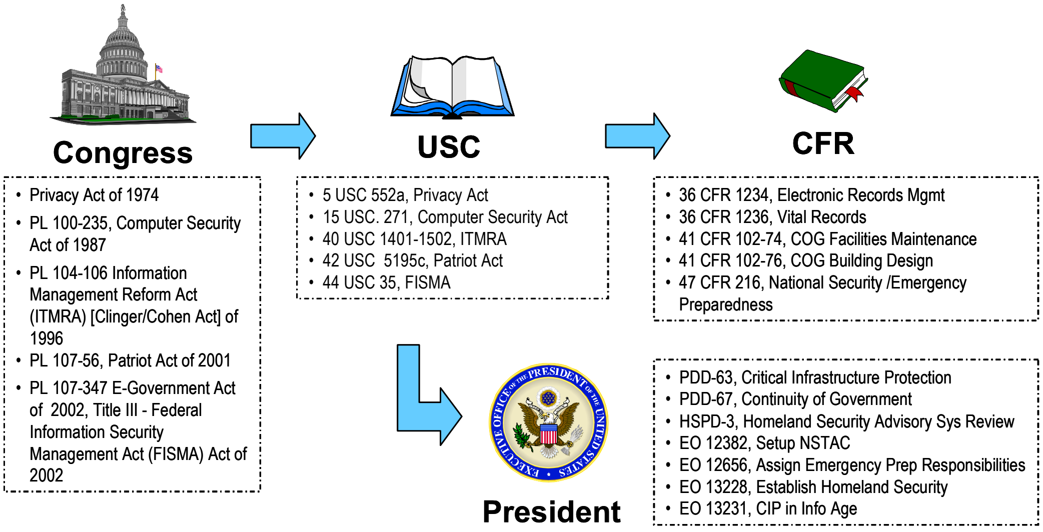

Congress
• Privacy Act of 1974
• PL 100-235, Computer Security Act of 1987
• PL 104-106 Information Management Reform Act (ITMRA) [Clinger/Cohen Act] of 1996
• PL 107-56, Patriot Act of 2001
• PL 107-347 E-Government Act of 2002, Title III - Federal Information Security Management Act (FISMA) Act of 2002
USC
• 5 USC 552a, Privacy Act
• 15 USC. 271, Computer Security Act
• 40 USC 1401-1502, ITMRA
• 42 USC 5195c, Patriot Act
• 44 USC 35, FISMA
CFR
• 36 CFR 1234, Electronic Records Mgmt
• 36 CFR 1236, Vital Records
• 41 CFR 102-74, COG Facilities Maintenance
• 41 CFR 102-76, COG Building Design
• 47 CFR 216, National Security /Emergency Preparedness
President
• PDD-63, Critical Infrastructure Protection
• PDD-67, Continuity of Government
• HSPD-3, Homeland Security Advisory Sys Review
• EO 12382, Setup NSTAC
• EO 12656, Assign Emergency Prep Responsibilities
• EO 13228, Establish Homeland Security
• EO 13231, CIP in Info Age

**Figure 6. Business Continuity Authorizing Documents**

As indicated in the previous chapter on generic flow of requirements, the documents shown above are sources for each department and agency in the Executive Branch to interpret and apply to their specific missions within the federal government. Figure 7 shows how the responsible departments and agencies have responded with Business Continuity-relevant directives and guides. The appendices contain detailed analyses of each document cited in this figure.

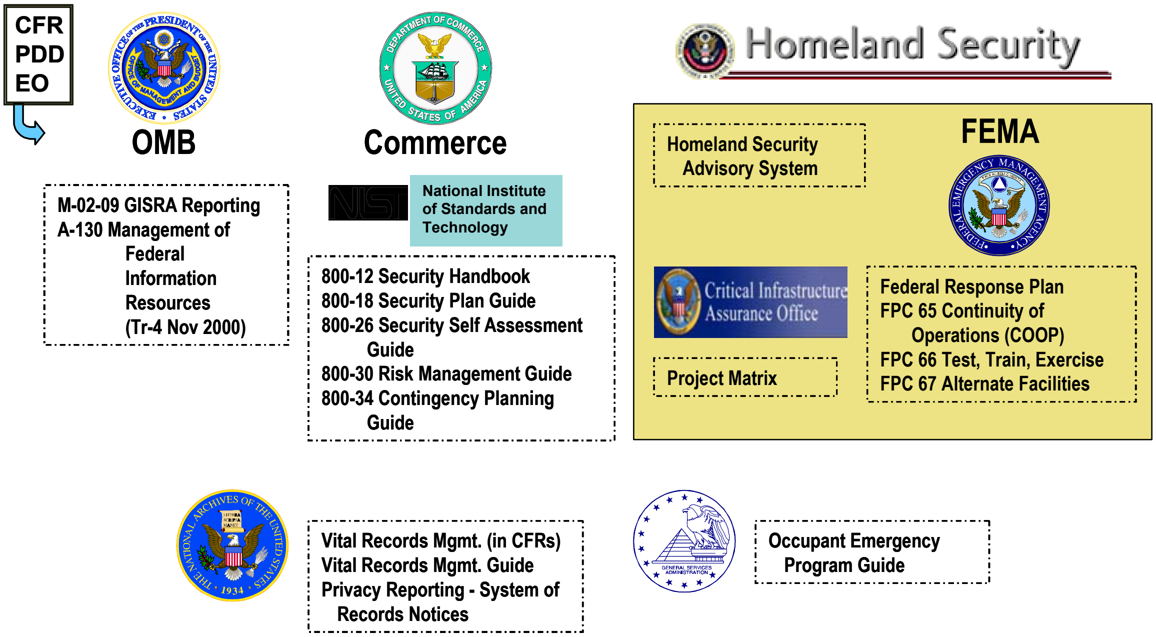

CFR
PDD
EO
OMB
M-02-09 GISRA Reporting
A-130 Management of Federal Information Resources (Tr-4 Nov 2000)
Commerce
NIST
National Institute of Standards and Technology
800-12 Security Handbook
800-18 Security Plan Guide
800-26 Security Self Assessment Guide
800-30 Risk Management Guide
800-34 Contingency Planning Guide
Homeland Security
Homeland Security Advisory System
FEMA
Critical Infrastructure Assurance Office
Project Matrix
Federal Response Plan
FPC 65 Continuity of Operations (COOP)
FPC 66 Test, Train, Exercise
FPC 67 Alternate Facilities
Vital Records Mgmt. (in CFRs)
Vital Records Mgmt. Guide
Privacy Reporting - System of Records Notices
Occupant Emergency Program Guide

**Figure 7. Executive Branch Applications of Business Continuity Responsibilities**

Another way of viewing the federal business continuity requirements is by seeing how they have evolved over time. Figure 8, the Genealogy of Business Continuity Planning Requirements, illustrates the sequence in which the source documents were developed.

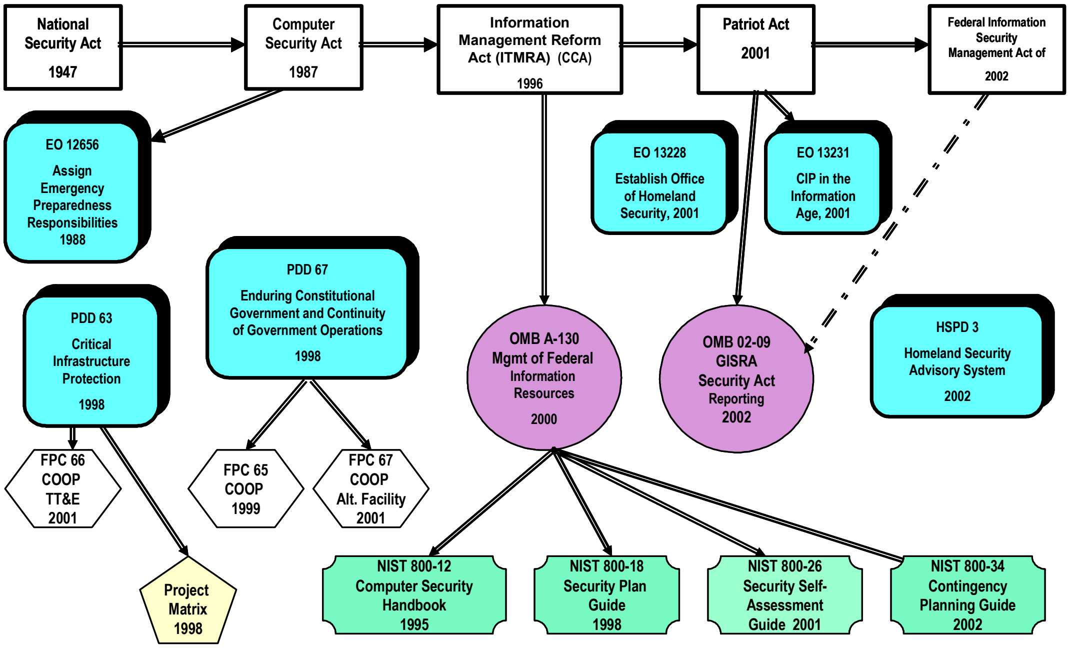

National Security Act 1947
Computer Security Act 1987
Information Management Reform Act (ITMRA) (CCA) 1996
Patriot Act 2001
Federal Information Security Management Act of 2002
EO 12656 Assign Emergency Preparedness Responsibilities 1988
EO 13228 Establish Office of Homeland Security, 2001
EO 13231 CIP in the Information Age, 2001
PDD 67 Enduring Constitutional Government and Continuity of Government Operations 1998
PDD 63 Critical Infrastructure Protection 1998
OMB A-130 Mgmt of Federal Information Resources 2000
OMB 02-09 GISRA Security Act Reporting 2002
HSPD 3 Homeland Security Advisory System 2002
FPC 66 COOP TT&E 2001
FPC 65 COOP 1999
FPC 67 COOP Alt. Facility 2001
Project Matrix 1998
NIST 800-12 Computer Security Handbook 1995
NIST 800-18 Security Plan Guide 1998
NIST 800-26 Security Self-Assessment Guide 2001
NIST 800-34 Contingency Planning Guide 2002

**Figure 8. Genealogy of Business Continuity Planning Requirements**

## 3.4 Department of Treasury Business Continuity Requirements

The Department of the Treasury provides guidance to its Bureaus in the form of Treasury Directives. It also sponsors a Treasury Critical Infrastructure Protection Working Group that is comprised of member from all Bureaus and Department Offices. The CIP working group has provided guidance that directly applies to Business Continuity requirements. MITRE's assessment of the specific Treasury documents reviewed is provided in Appendix B.

## 3.5 Internal Revenue Service Business Continuity Requirements

The Internal Revenue Manual (IRM) defines how all parts of the IRS are to function. IRM Section 25.10.1, Security Policy and Guidance, signed in January 2002, served as the primary IRS source for this report. While this section is not publicly available, relevant extracts are included in Appendix C.

## 3.6 External Auditor's Recommendations

MITRE also investigated recommendations from external auditing sources. General Accounting Office reports were searched and reviewed to identify any business continuity-relevant statements. Appendix D contains the results of that search and the MITRE analysis.

Another source of auditor's recommendations would be reports from the Treasury Inspector General for Tax Administration (TIGTA). MITRE identified several Limited Official Use (LOU) recommendations that may be applicable and the IRS should assess those documents independently. The list of TIGTA reports that were assessed separately by MITRE are provided in Appendix D.

# 4. Current Business and Government Business Continuity Best Practices

Business Continuity Management is a relatively new practice area. Growing out of the IT security area was a need to plan more than just "protect the systems," to being able to restore the systems, to being able to maintain business operations. The staff that had responsibility for IT security was called on initially to develop "disaster recovery plans." As the plans were developed, the need was recognized to include the business side of the organization in any recovery decisions. The development of new expertise and standardized processes was recognized by those involved, because they needed some way to represent their ideas and proposals to management for investment approval. Senior management needed to have some level of confidence in the requestor of the funding, and a clear understanding of what was being requested and why it was needed.

In response to these needs, two organizations were established:

- DRI International was founded in 1988 to provide a base of common knowledge in contingency planning, a rapidly growing industry at the time. DRII administers a global certification program for qualified business continuity and disaster recovery planners. *The Professional Practices for Business Continuity Planners* serves as the industry's best practices standard."[4]
- The Business Continuity Institute (BCI) was established in 1994 to provide opportunities to obtain guidance and support from fellow professionals. The Institute provides an internationally recognized status in relation to the individual's experience as a continuity practitioner.[5]

In 1997, DRII, together with BCI, published the Professional Practices for Business Continuity Planners[6] as the industry's international standard. MITRE used the May 2002 version of this standard as the basis for the approach and recommendations in this report.

## 4.1 Commercial Practices

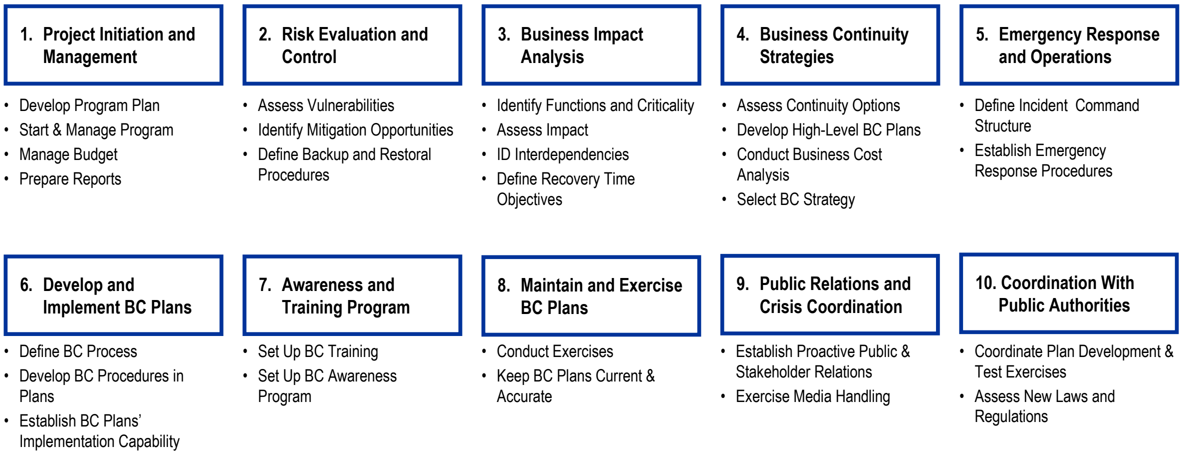
The Disaster Recovery Institute's *The Professional Practices for Business Continuity Planners*[7] establishes ten subject areas that should be addressed to properly plan and administer a business continuity program. Figure 9 presents the ten subject areas.

[4] DRII web site http://www.drii.org

[5] BCI web site http://www.thebci.org

[6] Available on DRII web site http://www.drii.org/ppcont

[7] Disaster Recovery Institute, International, *Professional Practices for Business Continuity Planners*, May 2002



**1. Project Initiation and Management**
- Develop Program Plan
- Start & Manage Program
- Manage Budget
- Prepare Reports

**2. Risk Evaluation and Control**
- Assess Vulnerabilities
- Identify Mitigation Opportunities
- Define Backup and Restoral Procedures

**3. Business Impact Analysis**
- Identify Functions and Criticality
- Assess Impact
- ID Interdependencies
- Define Recovery Time Objectives

**4. Business Continuity Strategies**
- Assess Continuity Options
- Develop High-Level BC Plans
- Conduct Business Cost Analysis
- Select BC Strategy

**5. Emergency Response and Operations**
- Define Incident Command Structure
- Establish Emergency Response Procedures

**6. Develop and Implement BC Plans**
- Define BC Process
- Develop BC Procedures in Plans
- Establish BC Plans' Implementation Capability

**7. Awareness and Training Program**
- Set Up BC Training
- Set Up BC Awareness Program

**8. Maintain and Exercise BC Plans**
- Conduct Exercises
- Keep BC Plans Current & Accurate

**9. Public Relations and Crisis Coordination**
- Establish Proactive Public & Stakeholder Relations
- Exercise Media Handling

**10. Coordination With Public Authorities**
- Coordinate Plan Development & Test Exercises
- Assess New Laws and Regulations

**Figure 9. Scope of Business Continuity Planning and Management**

Section 5 includes the details for each of the ten subject areas along with MITRE's recommended approach to address business continuity. The recommendations include additions to DRI's commercial standard shown here.

## 4.2 Governmental Standards

In June 2002, NIST issued Special Publication 800–34, *Contingency Planning Guide for Information Technology Systems*. NIST describes the scope of this document as follows:

> The document outlines planning principles that may be applied to a wide variety of incidents that could affect IT system operations. The scope includes minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in this document. Instead, the planning guide defines a process that may be followed for any IT system to identify planning requirements and develop an effective contingency plan for the disaster.
>
> The NIST planning guide does not address facility-level or organizational contingency planning, except for those issues required to restore information systems and their processing capabilities. Facility-level and organization contingency planning is normally the topic of a continuity of operations plan (COOP) rather than an IT contingency plan. In addition, this document does not address contingency planning for business processes because that subject would normally be addressed in business resumption or business continuity plan. Although information systems typically support business processes, the processes also depend on a variety of other resources and capabilities not associated with information systems. Continuity of operations, business resumption, and business

continuity plans are part of a suite of emergency management plans further described in Section 2.2.[8]

The NIST Guide describes the IT Contingency Planning process as the process to develop and maintain an effective IT contingency plan. The process presented here is common to all IT systems.

The document defines the following seven-step contingency process[9] that an agency may apply to develop and maintain a viable contingency planning program for their IT systems.

These seven progressive steps are designed to be integrated into each stage of the system development life cycle:

1. **Develop the contingency planning policy statement.** A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.

2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components. A template for developing the BIA is also provided to assist the user.

3. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life-cycle costs.

4. **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

6. **Plan testing, training, and exercises.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

7. **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.

The processes proposed by NIST are consistent with DRI subject areas: (2) Risk Evaluation and Control, (3) Business Impact Analysis, (4) Business Continuity Strategies, (6) Develop and Implement Business Continuity Plans, (7) Awareness and Training Program, and (8) Maintain and Exercise Business Continuity Plans. While there is some overlap with the DRI topics, as noted above, NIST's emphasis is the restoral of the IT systems, not the restoral of business processes.

[8] NIST 800-34 IT Contingency Planning Guide, page 3

[9] NIST 800-34, IT Contingency Planning Guide, page 14

One topic that NIST addresses that is missing from DRI's model is the need for establishing an enterprise policy, their number one item. MITRE has added this to the recommendations in this report.

Because the Business Continuity subject area is relatively new and NIST has only recently issued any guidance, many government employees in the field have turned to DRI for advice. As a result, most government disaster recovery planners are familiar with the DRI model.

## 4.3 Business Continuity Terminology and Timelines

When discussing business recovery, it is important to establish a consistent understanding of the timeline of expected events and use consistent terminology to communicate among the interested parties. Two terms have a significant importance in defining any business recovery: Recovery Time Objective (RTO) and Recovery Point Objective (RPO), as shown in Figure 10.

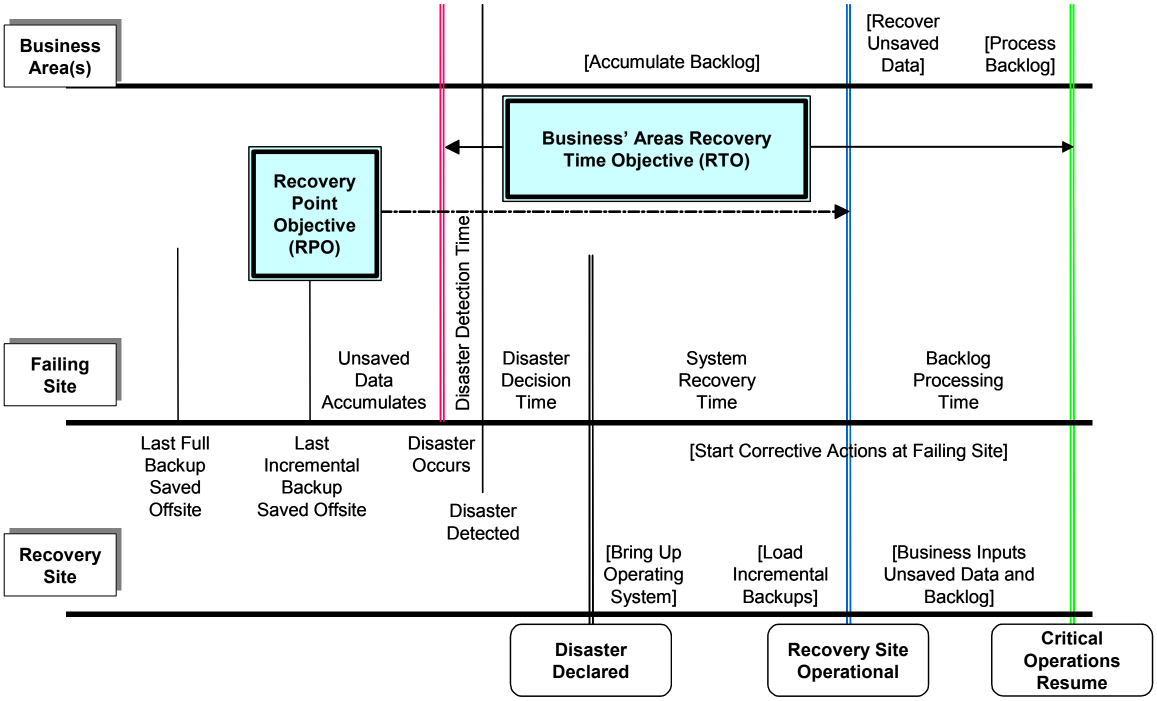

Business Area(s)
[Accumulate Backlog]
[Recover Unsaved Data]
[Process Backlog]
Business' Areas Recovery Time Objective (RTO)
Recovery Point Objective (RPO)
Disaster Detection Time
Failing Site
Unsaved Data Accumulates
Disaster Decision Time
System Recovery Time
Backlog Processing Time
Last Full Backup Saved Offsite
Last Incremental Backup Saved Offsite
Disaster Occurs
Disaster Detected
[Start Corrective Actions at Failing Site]
Recovery Site
[Bring Up Operating System]
[Load Incremental Backups]
[Business Inputs Unsaved Data and Backlog]
Disaster Declared
Recovery Site Operational
Critical Operations Resume

**Figure 10. Business Recovery Terminology and Timelines**

Recovery Time Objective is the duration that business determines it to be acceptable, or tolerable, for service to be halted. In general, there is a RTO for each business process. This is a financial and business decision that takes into consideration the potential loss of revenue and customer satisfaction versus the expense of reducing or virtually eliminating the outage. RTO could be specified in seconds, minutes, hours, days, or weeks. RTO starts when the disaster occurs and concludes when the business customers have service restored. RTO includes both the time it takes to make a decision and declare a disaster, plus the time for system recovery at that alternate location (to Recovery Site Operational). It may also include the time to process any backlog if customer service is inhibited during this time (to Critical Operations Resume).

Recovery Point Objective is a state, or point in time, at which a system will be restarted. When recovery at an alternate site is initiated, the hardware and operating programs must first be brought to a functioning condition. The next step is to make the data used by the system accessible by the programs. The currency of this data is the RPO. Historically, a full backup of all data will be taken periodically and stored at an off-site location. On a more frequent basis, changes to that version of data will be made incrementally and also stored offsite. When recovery occurs, both sets of data are loaded into the alternate location's systems. The more frequently these incremental changes are stored offsite, the more expensive the daily operation becomes. A business decision must be made to trade off which data is the most critical and how much data the business can afford to lose. The RPO captures that business decision. RPO is usually specified in time increments representing how often data changes are stored offsite. Mission-critical data may be saved after each transaction, or specified in minutes, hours, or days.

When business impact analyses are done, the analysts investigate various RTO and RPO parameters to determine impact. Business strategies are developed to meet agreed upon desired RTOs and RPOs.

## 4.4 Survey of Current BCP Practice

This section provides a survey of a small, but hopefully representative, sample of the commercial literature readily available on the Internet concerning the current state of Business Continuity Planning and Management. Each subsection that follows contains a summary of a related article or report. The source of the material and the author's name, if known, are identified. The table at the end of each paragraph indicates how the article or report can be applied to the ten subject areas in the DRI business continuity model.

### 4.4.1 Project Initiation and Management

In an article entitled "Project Initiation and Management," David Honour reports that business continuity planning is a project with a beginning and an end, while business continuity management is an ongoing process with no determined end. The first step in business continuity planning—project initiation and management—is concerned with getting the project off the ground.

The first critical aspect of project initiation is obtaining the support of the senior management of the organization. If they are not on board, the project is doomed before it has even been started. Senior management needs to understand the reasons for the business continuity plan and the benefit that the company will obtain from having it. A key consideration when developing the business case is to enlist the help of a project sponsor to gain access to the senior managers/board. A project sponsor is someone with influence who is receptive and sympathetic to the idea of business continuity planning and who facilitates access to the senior managers.

Source: www.globalcontinuity.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.2 “Not Much New In Business Continuity. Not Even Budgets”

According to an article by David Berlind entitled “Not much new in business continuity. Not even budgets,” the level of participation in BCP appears to be low. Fewer than 25% of Global 2000 enterprises have invested in comprehensive business continuity planning and only 50% of those have fully tested their plans. A difficult issue facing IT managers is how much money to devote to DR. Currently, the average is about 4% of the overall IT budget; however, the best approach seems to be to quantify the cost of downtime and set the objectives for RTO and RPO accordingly.

Source: www.techupdate.zdnet.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| ✓ | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.3 Disaster Recovery Then and Now

In “Disaster Recovery Then And Now, “John Fontana and Deni Connor report that Gartner estimates that 85% of large organizations have some sort of disaster recovery plan, but that only 25% of them have a broader business continuity plan, and only 10–15% of them are up to date. Corporations have typically focused on IT at the expense of the rest of the business.

Source: www.nwfusion.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.4 Invocation Survey—Final Results

On Globalcontinuity.com, a web portal for business continuity and disaster recovery, reports in "Invocation Survey—Final Results" that approximately 30% of the organizations that responded to a survey had experienced at least one invocation of their BC plans. The most common causes were flooding and power outage. The respondents believed that approximately 85% of BC plans achieved their recovery time objectives.

Source: www.globalcontinuity.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.5 Survey: More than One-Third of Organizations Have Activated Their Business Continuity Plans

Strohl Systems Online Newsroom released the results of a recent survey of business continuity professionals completed in August 2002 by Strohl Systems and *Contingency Planning and Management* magazine. The survey found that 38% of the responding organizations had activated their business continuity plan, while 57% had not activated their plan and 5% did not have a plan.

Source: www.strohlsystems.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | ✓ | 6 | Develop & Implement BC Plans |
|  | 2 | Risk Evaluation & Control |  | 7 | Awareness & Training Program |
|  | 3 | Business Impact Analysis |  | 8 | Maintain & Exercise BC Plans |
|  | 4 | Business Continuity Strategies |  | 9 | Public Relations and Crisis Coordination |
|  | 5 | Emergency Response & Operations |  | 10 | Coordination with Public Authorities |

### 4.4.6 Survey: Majority of Organizations Have Had BCP Program for Less Than Five Years

Strohl Systems Online Newsroom released the results of a recent survey of business continuity planning professionals. The survey found that 64% of responding organizations have a BC plan that has been in place for 5 years or less. Thirty-six percent of the respondents indicated the IT department is in charge of BC planning in their organization.

Source: www.strohlsystems.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management |  | 6 | Develop & Implement BC Plans |
|  | 2 | Risk Evaluation & Control |  | 7 | Awareness & Training Program |
|  | 3 | Business Impact Analysis |  | 8 | Maintain & Exercise BC Plans |
|  | 4 | Business Continuity Strategies |  | 9 | Public Relations and Crisis Coordination |
|  | 5 | Emergency Response & Operations |  | 10 | Coordination with Public Authorities |

### 4.4.7 Three Out of Four Organizations Have Reviewed Their Business Continuity Plan since September 11

Strohl Systems Online Newsroom released the results of a recent survey of business continuity professionals, which found that 76% of the respondents indicated that their organization has reviewed their business continuity plans since September 11, 2001. Fifty-two percent of those surveyed made some changes to their plan, while 10% completely overhauled their plans, and 14% reviewed their plans but did not make any changes.

Source: www.strohlsystems.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management |  | 6 | Develop & Implement BC Plans |
|  | 2 | Risk Evaluation & Control |  | 7 | Awareness & Training Program |
|  | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
|  | 4 | Business Continuity Strategies |  | 9 | Public Relations and Crisis Coordination |
|  | 5 | Emergency Response & Operations |  | 10 | Coordination with Public Authorities |

### 4.4.8 High-Profile Evacuation

In an article entitled "High-Profile Evacuation," Victoria Hardy outlines how the 1993 bombing of the World Trade Center could well have saved lives in the 2001 disaster. More than 18,000 people evacuated safely from the World Trade Center complex in the 1 hour and 42 minutes between the first jet impact and the second building collapse. The success of the evacuation could have been due to improvements that were made to the buildings after the 1993 bombing. Some of the improvements after the 1993 bombing include:

- Reflective paint was added to all doors, stairs, and railings to guide people in the event of poor visibility
- A building-wide speaker system was installed to communicate with people at the exit locations
- Every disabled person was given an evacuation chair
- Emergency lighting in the stairwells was set up on backup battery power
- Evacuation drills were held every 6 months.

Source: www.infolink.com.au

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
|  | 1 | Project Initiation & Management |  | 6 | Develop & Implement BC Plans |
|  | 2 | Risk Evaluation & Control |  | 7 | Awareness & Training Program |
|  | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
|  | 4 | Business Continuity Strategies | ✓ | 9 | Public Relations and Crisis Coordination |
| ✓ | 5 | Emergency Response & Operations |  | 10 | Coordination with Public Authorities |

### 4.4.9 Business Continuity Planning Practices Explored

In "Business Continuity Planning Practices Explore," Globalcontinuity.com reports on a survey on business continuity and disaster recovery planning that was designed to gauge the amount of change and focus in business continuity planning over the last year. Nearly 85% of the respondents said their companies currently have business continuity and disaster recovery plans in place, compared with 73% who said their companies had plans in place prior to September 11, 2001.

The study also considered responsibility for business continuity efforts. In nearly 34 % of companies, the CIO was responsible, while 21% gave the job to the CEO. Less than 12 % of respondents identified a specifically appointed head of security for business continuity planning. Some business continuity planners believe that appointing a specific individual or office to deal with business continuity issues shows a company's commitment to heading off problems and ensuring that the plan stays actionable and current.

Source: www.globalcontinuity.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.10 BCM Maturity Model

In an article entitled "BCM Maturity Model," Virtual Corporation reports that it has developed the BCM Maturity Model, analogous to the Software Engineering Institute (SEI) Capability Maturity Model (CMM) ® model, as an objective means of measuring the effectiveness of Business Continuity implementations. This goal is achieved through defining the evolutionary path that Business Continuity implementations follow as they mature over time coupled with baseline data on the BCM Maturity of organizations across industry, geographic, and other relevant boundaries.

In this six-level BCM model, levels one through three represent organizations that have not yet completed the necessary program basics needed to launch a sustainable enterprise BCM Program. Levels four through six represent the evolutionary path of the maturing enterprise BCM Program. At each level, companies may progress to the next level or, if they lose momentum, fall back one or more levels. As with any business process, if the supporting infrastructure is removed or significantly diminished, the effectiveness of the BCM Program will deteriorate and with it the company's state of preparedness.

Source: www.virtual-corp.net

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.11 Disasters—Plan For Your People Above All Else

Peter Power reports, in an article entitled “Disasters—Plan For Your People Above All Else,” that too many business continuity and crisis planners ignore human emotion. They tend to see the processes they are dealing with as highly systematic, cerebral, and conscious. However, emotion clutters up the processing of information.

One of the greatest lessons from September 11 was that people are more important than processes: business continuity is meaningless unless it considers the protection of human as well as technological resources.

Source: www.globalcontinuity.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | ✓ | 9 | Public Relations and Crisis Coordination |
| ✓ | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.12 Wider than IT

Gary Leather makes the case in an article entitled “Wider than IT” that there are many companies whose most critical assets are not IT systems, but people. However, the business continuity function is, in the majority of businesses, the responsibility of the IT department. Therefore, in many cases, the funding for business continuity comes out of the IT budget and tends to focus on IT security and continuity systems. This situation needs to be changed if the practice of business continuity is to progress.

Source: www.thebci.org

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.13 Benchmark Report: BCP in 2002

In an article entitled "Benchmark Report: BCP in 2002," Andy Hagg reports on the results of the 2002 CPM/KPMG Business Continuity Benchmark Survey. Ten thousand survey kits were mailed out and 624 responses were received from the U.S. and Canadian circulation of *Contingency Planning & Management* magazine.

The survey indicates that companies are considering a broader scope of causes of business disruptions, indicating that companies are recognizing the complexities of business and are seeking to mitigate disruption from all fronts.

A key goal for business continuity plans is the recovery time objective. The RTO continues to decrease in size for most of the survey respondents. Over 73% report RTOs of less than 24 hours. Fewer than half of the respondents said their RTOs were met after their most recent interruption and fewer than 35% were able to claim success at maintaining their service levels.

Source: www.contingencyplanning.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | | 6 | Develop & Implement BC Plans |
| | 2 | Risk Evaluation & Control | | 7 | Awareness & Training Program |
| ✓ | 3 | Business Impact Analysis | | 8 | Maintain & Exercise BC Plans |
| ✓ | 4 | Business Continuity Strategies | | 9 | Public Relations and Crisis Coordination |
| | 5 | Emergency Response & Operations | | 10 | Coordination with Public Authorities |

### 4.4.14 Looking Back for the Future

David Davies details the risk management lessons learned from September 11 in an article entitled "Looking Back for the Future." Some of the key findings include:

- Highly detailed plans were less effective, because no disaster turns out exactly as expected. The recovery strategy has to be rapidly assembled and adjusted dynamically as new information emerges.
- Many employees did not have copy plans at home

- Some plans were based on optimistic scenarios
- Some plans had not been updated to reflect recent changes to the business
- People can be lost, as well as property
- The effects of trauma can be as great as physical injury
- Trauma can destroy leadership ability
- A public relations crisis plan should be created and be capable of being invoked in parallel with the disaster recovery and business continuity plans.

Source: www.globalcontinuity.com

**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | ✓ | 6 | Develop & Implement BC Plans |
| ✓ | 2 | Risk Evaluation & Control | ✓ | 7 | Awareness & Training Program |
|  | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
|  | 4 | Business Continuity Strategies | ✓ | 9 | Public Relations and Crisis Coordination |
| ✓ | 5 | Emergency Response & Operations |  | 10 | Coordination with Public Authorities |

### 4.4.15 U.S. Financial Institutions Face Tough New Business Continuity Regulations

In an article entitled “U.S. Financial Institutions Face Tough New Business Continuity Regulations,” Globalcontinuity.com reports that four financial services regulatory agencies have issued a “Draft interagency white paper on sound practices to strengthen the resilience of the US Financial system.” The four agencies are the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the New York Banking Department.

If the white paper is adopted, regulated companies will have to show that their business continuity plans will allow the recovery of business processes and functions “sufficient to complete critical activities by the end of each business day” even in the event of a wide-area disaster.

The draft white paper provides that firms that play significant roles in financial markets should, at a minimum, plan to recover on the same business day the critical activities they perform that support the recovery of critical markets. The recovery time target for these firms is moving toward no later than 4 hours after the event.

Regulated firms should have backup arrangements with sufficient out of region staff, equipment, and data to recovery their critical activities within the recovery time objectives. Backup locations should not be dependent on the same labor pool or infrastructure components used by the primary site, and their respective labor pools should not both be vulnerable to simultaneous evacuation or inaccessibility.

Regulated firms should routinely use or test their individual internal recovery and resumption arrangements for required connectivity, functionality, and volume capacity.

The white paper can be read at:
www.federalreserve.gov/boarddocs/press/bcreg/2002/20020830/attachment.pdf

Source: www.globalcontinuity.com

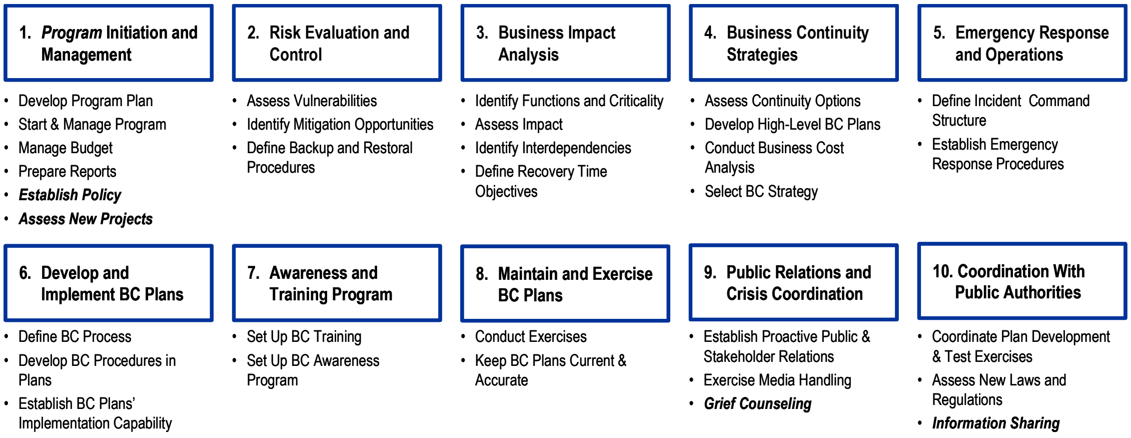
**Subject Areas for Application of Article**

| ✓ | # | Subject Area | ✓ | # | Subject Area |
|---|---|---|---|---|---|
| ✓ | 1 | Project Initiation & Management | ✓ | 6 | Develop & Implement BC Plans |
| ✓ | 2 | Risk Evaluation & Control | ✓ | 7 | Awareness & Training Program |
| ✓ | 3 | Business Impact Analysis | ✓ | 8 | Maintain & Exercise BC Plans |
| ✓ | 4 | Business Continuity Strategies | ✓ | 9 | Public Relations and Crisis Coordination |
| ✓ | 5 | Emergency Response & Operations | ✓ | 10 | Coordination with Public Authorities |

# 5. Recommended Approach to Address Business Continuity

MITRE recommends using the DRI model, with a few additions as noted in italics in Figure 11 to address the specific concerns of the federal government that are not present in the commercial model. The DRI model provides a suitable framework for associating existing federal requirements and advisories to common BC subject areas. The appendices contain the detailed results of MITRE's analysis of the requirements. Each requirement or advisory and source is collected under a subject area. The complete list provides the business continuity functional requirements that the IRS and other federal agencies should address.

It is intended that this composite list of requirements will be used to conduct a business continuity "as is" review of the Enterprise Architecture to ensure that the agency is meeting all BC requirements.



**1. *Program* Initiation and Management**

- Develop Program Plan
- Start & Manage Program
- Manage Budget
- Prepare Reports
- ***Establish Policy***
- ***Assess New Projects***

**2. Risk Evaluation and Control**

- Assess Vulnerabilities
- Identify Mitigation Opportunities
- Define Backup and Restoral Procedures

**3. Business Impact Analysis**

- Identify Functions and Criticality
- Assess Impact
- Identify Interdependencies
- Define Recovery Time Objectives

**4. Business Continuity Strategies**

- Assess Continuity Options
- Develop High-Level BC Plans
- Conduct Business Cost Analysis
- Select BC Strategy

**5. Emergency Response and Operations**

- Define Incident Command Structure
- Establish Emergency Response Procedures

**6. Develop and Implement BC Plans**

- Define BC Process
- Develop BC Procedures in Plans
- Establish BC Plans' Implementation Capability

**7. Awareness and Training Program**

- Set Up BC Training
- Set Up BC Awareness Program

**8. Maintain and Exercise BC Plans**

- Conduct Exercises
- Keep BC Plans Current & Accurate

**9. Public Relations and Crisis Coordination**

- Establish Proactive Public & Stakeholder Relations
- Exercise Media Handling
- ***Grief Counseling***

**10. Coordination With Public Authorities**

- Coordinate Plan Development & Test Exercises
- Assess New Laws and Regulations
- ***Information Sharing***

Source: *Professional Practices for Business Continuity Planners*, *Modified,* DRI International, May 2002

Note: *Italics* represent proposed changes to the DRI model to include Federal Government needs.

**Figure 11. Federal Government Approach to Managing Business Continuity**

## 5.1 Program Initiation and Management

One change proposed to the DRI model is to increase the scope from managing a project to that of managing a program, recognizing that scope of the effort will necessitate organizing several projects.

The following topics need to be addressed to successfully start and manage a Business Continuity Program:

- Find a Champion at the Senior Leadership Level
- Lead Stakeholders in Defining Objectives, Policies, and Critical Success Factors
- Coordinate and Organize/Manage the BCP Program
- Oversee the BCP Program Through Effective Control Methods and Change Management

- Present (Sell) the Program to Management and Staff
- Develop Program Plan and Budget
- Define and Recommend Program Structure and Management
- Manage the Program
- *Establish Policy*[10]
- Assess new projects.

## 5.2 Risk Evaluation and Control

The following topics need to be addressed to successfully start and manage risk evaluation and control from a business continuity perspective:

- Understand Loss Potentials
- Determine Organization's Vulnerability to Loss Potentials
- Identify Controls and Safeguards to Prevent or Minimize Effect of Loss Potential [Mitigation opportunities]
- Evaluate, Select, and Use Appropriate Risk Analysis Methodologies and Tools
- Identify and Implement Information Gathering Activities
- Evaluate Effectiveness of Controls and Safeguards
- Develop Risk Evaluation and Determine Needed Controls
- Address Security Exposures
- Determine Backup and Restoral Procedures.

## 5.3 Business Impact Analysis

The following topics need to be addressed to successfully start and manage business impact analysis from a business continuity perspective:

- Identify Organizational Functions
- Define Criticality of Business Functions and Records, Prioritize
- Assess Effects of Disruptions, Loss Exposure, and Business Impact
- Determine Recovery Timeframes [RTO]
- Identify Business Processes Interdependencies
- Identify Information and Resource Requirements for Recovery

[10] The items in italic are MITRE-recommended changes to the DRI process.

- Document Business Impact Analysis results for each function considered
- What will it cost the organization if the function is lost?
- Who is impacted?

## 5.4 Business Continuity Strategies

The following topics need to be addressed to successfully start and manage business continuity strategies from a business continuity perspective:

- Identify Business Continuity Strategy Requirements
- Determine Possible Alternative Strategies Against BIA
- Develop High Level Implementation Plans for Best Strategy Options
- Select Alternate Site(s) and Off-site Storage
- Understand Contractual Agreements for Business Continuity Services
- Prepare Cost, Benefit Analysis of Strategies
- Select Strategy for Implementation
- Integrate Business Continuity Plans with Enterprise Plans
- Develop Business Unit Plans for How They Will Respond
- Understand Communications Requirements Amongst Users.

## 5.5 Emergency Response and Operations

The following topics need to be addressed to successfully establish and maintain an ability to quickly respond to an incident:

- Identify Components of Emergency Response Procedures
- Establish Reporting Procedures
- Manage Pre-incident Preparations
- Perform Emergency Actions
- Perform Facility Stabilization
- Perform Damage Mitigation
- Determine Testing Procedures and Responsibilities
- Develop Detailed Emergency Response Procedures
- Define the Command and Control Requirements and Procedures
- Develop Emergency Response and Triage Procedures

- Develop Plans for Salvage and Restoration.

## 5.6 Develop and Implement Business Continuity Plans

The following topics need to be addressed to successfully develop plans to quickly recovery from an incident:

- Define Recovery Management and Control Requirements
  Define Disaster and Approach to Recovery [phases]
  Define Recovery Teams and Command Center
- Develop Procedures to Ensure Business Continuity
  Identify Organizational Information
  Develop Protection and Replication Strategies
  Determine How to Conduct Information Recovery
  Define Optional Business Methods
- Define How to Conduct Damage Assessment
- Determine Critical Resource Acquisition Needs and Plans
- Define Security Maintenance Procedures
- Address Human Resource and Personnel Considerations
- Document Business Continuity Plan
  Develop General Introduction or Overview [Incident Mgmt.]
  Plan Activation
  Team Organization
  Policy Statement
  Emergency Operations Center
  Develop Administration Plan
  Resource Management, media coordinator, other liaisons
  Vital Record Management
  Admin Department Procedures.

As part of the planning effort it is necessary to establish a uniform incident command structure that can respond to any type of major incident. The Fire and Rescue organizations have developed an Incident Command Structure that has been adapted by FEMA. That structure is presented in Figure 12, Incident Command Structure. This illustration has been modified to identify the role the National Treasury Employee's Union plays in coordinating an incident response. While each box identifies a subject to be addressed as a result of an incident, smaller locations may utilize staff to fill several functions.

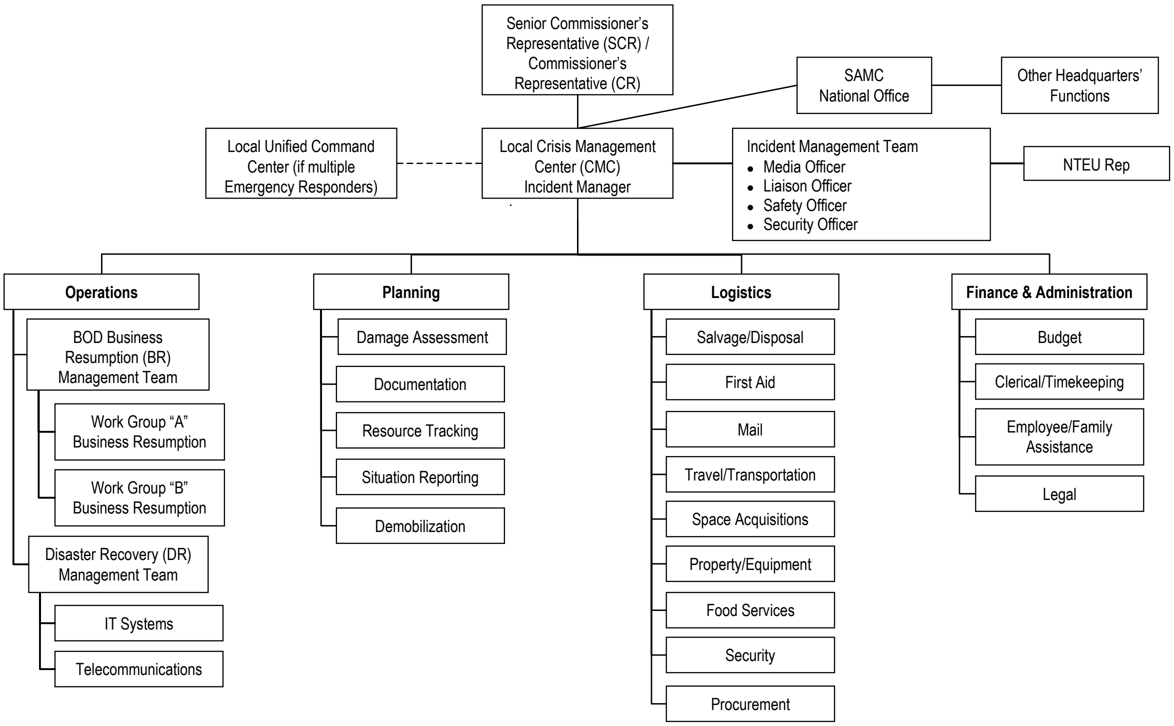


**Figure 12. Incident Command Structure**

## 5.7 Awareness and Training Program

The following topics need to be addressed to successfully establish and maintain a Business Continuity awareness and training program:

- Establish Objectives and Components of Training Program
- Identify Functional Training Requirements
- Develop Training Methodology
- Develop Awareness Program
- Acquire or Develop Training Aids
- Identify External Training Opportunities
- Identify Vehicles for Corporate Awareness

## 5.8 Maintain and Exercise Business Continuity Plans

The following topics need to be addressed to successfully maintain and exercise the business continuity plans. The purpose of this subject area is to ensure that all staff understand their roles and responsibilities during an incident and have experience fulfilling those responsibilities.

- Pre-plan the Exercises
- Coordinate the Exercises

- Evaluate the Exercise Plans
- Exercise the Plans
- Document the Results
- Evaluate the Results
- Update the Plan
- Report Results/Evaluation to Management
- Understand Strategic Directions of the Business
- Conduct Strategic Planning Meetings
- Coordinate Plan Maintenance
- Assist in Establishing Audit Program for the Business Continuity Plan

## 5.9 Public Relations and Crisis Coordination

The following topics need to be addressed to successfully coordinate activities during a crisis and ensure that communications about the incident is concise, accurate, and appropriate for the intended audience:

- Identify Components of Proactive Public Relations Program
- Identify External Agencies with Which Liaison is Required
- Identify Stakeholder Groups and Establish Essential Communications Plans
- Establish and Exercise Media Handling Plans
- *Manage Grief Counseling*
- Support External Audits

## 5.10 Coordination with Public Authorities

The following topics need to be addressed to successfully coordinate activities during a crisis with other federal, state, and local authorities:

- Coordinate Emergency Preparations, Response, Recovery, Resumption, and Restoration Procedures with Public Authorities
- Establish Liaison Procedures for Emergency/Disaster Scenarios
- Maintain Current Knowledge of Laws and Regulations Concerning Emergency Procedures
- Support Information Sharing Activities

# 6. IRS Business Continuity Requirements

This section provides a composite list of the business continuity-applicable requirements that were identified by MITRE's review and analysis of the documents listed in the List of References. Detailed descriptions of those documents that contained applicable material are provided in the Appendices and summarized in the following tables. The number symbol (#) identifies which specific entry in the appendix table captures the requirement.

This section presents a set of two tables for each of the ten DRI subject areas separated by sections. The first table of each section identifies the "hard" requirements which every federal agency/bureau is expected to support. The second table contains statements that present "advisory" type information that while not prescriptive in nature, should be reviewed and considered by anyone working in the subject area.

## 6.1 Program Initiation and Management

Table 1. Requirements for Program Initiation and Management

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 1. | Computer systems require Security Plans | Computer Security Act (3) |
| 2. | Establish a plan for the security and privacy of each Federal computer system | Computer Security Act (6) |
| 3. | Ensure that the information security policies, procedures, and practices are adequate | Clinger/Cohen (4) |
| 4. | Minimize Critical Infrastructure disruptions | Patriot Act (2) |
| 5. | Federal agency responsibilities<br>The head of each agency shall be responsible for providing information security protections | FISMA (2) |
| 6. | Each agency shall develop, document, and implement an agency wide information security program …, that includes:<br>…(2) policies and procedures | FISMA (4) |
| 7. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. | FISMA (9) |
| 8. | Agencies shall conduct a vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure. | PDD-63 (10) |
| 9. | Homeland Security Advisory System shall be binding on the executive branch | HSPD-3 (2) |
| 10. | HSPD Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. | HSPD-3 (3) |

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 11. | All Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system | HSPD-3 (4) |
| 12. | Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. | HSPD-3 (7) |
| 13. | Agencies shall identify programs that contribute to the Administration's strategy for homeland security and, in the development of the President's annual budget submission. The Office of Homeland Security shall review and provide advice to the heads of departments and agencies for such programs. | EO 13228 (18) |
| 14. | Agencies are authorized, to the extent permitted by law, to detail or assign personnel of such departments and agencies to the Office of Homeland Security upon request | EO 13228 (19) |
| 15. | The CIP program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. | EO 13231 (2) |
| 16. | Agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately addresses these mission areas. | EO 13231 (6) |
| 17. | Coordinate [Recruitment, Retention, and Training] programs to ensure that government employees with responsibilities for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, are adequately trained and evaluated | EO 13231 (12) |
| 18. | Heads of agencies are responsible for the vital records program. | 36CFR1236 (3) |
| 19. | The IT Capital Plan must include a component that demonstrates that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance. | OMB A-130 (6) |
| 20. | Information systems must identify and offer security protections; | OMB A-130 (7) |
| 21. | Agency budget requests should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets. | OMB M-02-09 (2) |
| 22. | Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. [for GISRA reporting] | OMB M-02-09 (3) |

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 23. | Agencies should measure and report [GISRA] how has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities | OMB M-02-09 (4) |
| 24. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 25. | Policy is needed to create and document the organization's approach to contingency planning. The policy should explicitly assign responsibilities. | NIST SP 800-12 (8) |
| 26. | Contingency plans must be based on a clearly defined policy | NIST SP 800-34 (4) |
| 27. | The Occupant Emergency Plan Designated Official (DO) must maintain an inventory of hazardous materials used in chemical laboratories and hazardous material storage areas in the building. | GSA OEP Guide (10) |
| 28. | Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. | GAO-00-295, INFORMATION SECURITY (2) |
| 29. | Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. | GAO-01-1168T, Critical Infrastructure Protection (8) |
| 30. | The Bureau Chief Information Officers, shall designate a point of contact to coordinate all policy issues related to information systems security (including computer security, telecommunications security, operational security (threats/vulnerability assessments), emissions security (TEMPEST), certificate management, electronic authentication, disaster recovery and continuity of operations for systems, and critical infrastructure protection related to cyber threats). | TD-71-10 (1) |
| 31. | The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to:<br>Ensure development, and within available appropriations, fund programs that adequately address these [CIP support] mission areas. | Treasury Critical Infrastructure Protection Plan (6) |
| 32. | Each Departmental Office and Bureau will develop its own CIP Management Plan following the guidance provided in this plan and the Treasury CIP Implementation Plan. In each such CIP Management Plan, the Departmental Office and Bureau will address the complete set of CIP-related goals, which include governance, risk management, critical asset management, threat assessment, vulnerability/risk assessment, business continuity planning and management, incident reporting and handling, and training and awareness. | Treasury Critical Infrastructure Protection Plan (8) |
| 33. | Departmental Office and Bureau heads shall:<br>Ensure the development of Departmental Office and Bureau CIP Management Plans that address all required information specified in the Treasury CIP Implementation Plan.<br>Retain overall responsibility for the assurance of critical infrastructure subject to their respective authority or control. | Treasury Critical Infrastructure Protection Plan (9) |

| # | 6.1 Requirement Description | Source |
|---|---|---|
| | Provide for increased reliability, security and redundancy; plan for critical infrastructure asset disruption or loss and subsequent restoration; and develop systems that are less dependent upon vulnerable infrastructures and systems. Provide for supplemental, integrated, infrastructure vulnerability assessment and assurance capability when requirements exceed internal capabilities.<br>Provide a senior representative(s) to the TIPP (Treasury Infrastructure Protection Panel).<br>As requested, provide staff or contractual assistance to support the TIPP and comply with other requirements of the Treasury security organization in accordance with TD P 71-10 and this TCIPP. | |
| 34. | Departmental Office and Bureau heads shall:<br>Conduct an annual review of their respective critical infrastructure. This review shall include the validation of data on facilities and their dependencies, an examination of facility and tenant plans for increasing reliability, reducing vulnerabilities, and mitigating hazards to and restoration of critical infrastructure.<br>Carry out industrial security program requirements specified in TD P 71-10.<br>Provide data requested by the Treasury security organization on the status of their respective critical infrastructure. | Treasury Critical Infrastructure Protection Plan (10) |
| 35. | Departmental Office and Bureau heads shall:<br>Establish and maintain a CIP awareness and training program. | Treasury Critical Infrastructure Protection Plan (11) |
| 36. | The Chief, Information Technology Services shall ensure the capability to implement the IRS business continuity planning program policy. | IRM 25.10.1 (1) |
| 37. | Business Continuity Plan resource requirements will be identified to support the recovery of critical processes and applications. | IRM 25.10.1 (27) |
| 38. | The Director, Office of Security is responsible for managing core security operations, which include the systems security certification and accreditation process, computer security incident response capabilities (CSIRC), Critical Infrastructure Protection (CIP) program, security awareness program, and existing and planned business resumption/disaster recovery/continuity of operations capabilities. | IRM 25.10.1 (2) |
| 39. | The Director, Office of Cyber Security is responsible for working with Information Technology Services (ITS) Operations and business units to identify existing and planned business resumption/disaster recovery/continuity of operations capabilities, including the establishment of executable/tested business resumption plans. | IRM 25.10.1 (3) |
| 40. | The Commissioner of the IRS shall:<br>a) designate senior management officials to establish and manage the Business Continuity Planning Program for the IRS, and b) establish policy and ensure compliance with those directives identified in this section. | IRM 25.10.1 (12) |

| # | 6.1 Requirement Description | Source |
|---|---|---|
| 41. | The senior executive responsible for an IRS business function shall initiate and ensure that the Business Continuity Planning Program policy established by the Commissioner is followed, and delegate implementation of the Business Continuity Program to Heads of Office. The senior executive shall also cooperate among various business units to develop, maintain, and validate effective, comprehensive plans. | IRM 25.10.1 (13) |
| 42. | Each Head of Office shall:<br>a. ensure an Executive Steering Committee is established to make site-specific policy/business decisions regarding development of the site Business Continuity Plan; | IRM 25.10.1 (14) |
| 43. | Each Head of Office shall:<br>e. ensure that Performance Measures are followed for the planning, implementation, testing, review, and maintenance of Business Continuity Plans for all critical business functions; | IRM 25.10.1 (18) |
| 44. | Business Continuity Plan resource requirements will be identified to support the recovery of critical processes and applications. | IRM 25.10.1 (27) |

### Table 2. Advisories and Guides for Program Initiation and Management

| # | 6.1 Advisory Description | Source |
|---|---|---|
| 1. | National Policy is to maintain the ability to protect the nation’s critical infrastructures from intentional acts | PDD-63 (2) |
| 2. | There shall be a senior executive branch board [CIPB] to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:<br>(b) protection of Federal departments’ and agencies’ critical infrastructure; | EO 13231 (4) |
| 3. | The [CIPB] Board shall recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.<br>NOTE: Treasury is on the Board, as such it is assumed that IRS will be tasked to represent their critical infrastructure assets to [or for] the Department of Treasury. | EO 13231 (7) |
| 4. | The NIPC will advise departments and agencies on legislation relating to protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. | EO 13231 (13) |
| 5. | Agencies shall make all reasonable efforts to keep the [NIPC] Chair fully informed in a timely manner, and to the greatest extent permitted by law, of all programs and issues within the purview of the Board. The Chair, in consultation with the Board, may propose policies and programs to appropriate officials to ensure the protection of the Nation’s information systems for critical infrastructure | EO 13231 (14) |
| 6. | Vital Records Definitions. | 36CFR1236 (4) |

| # | 6.1 Advisory Description | Source |
|---|---|---|
| 7. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 8. | Agencies must plan in an integrated manner for managing information throughout its life cycle | OMB A-130 (2) |
| 9. | Each agency should develop a vital records plan | NARA Vital Records Guide (5) |
| 10. | Security Program Management. Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. | GAO-01-1168T, Critical Infrastructure Protection (1) |
| 11. | Other critical success factors identified included:<br>(1) establishing effective and appropriately secure communication mechanisms, such as regular meetings and secure Web sites, (2) obtaining the support of senior managers at member organizations regarding the sharing of potentially sensitive member information and the commitment of resources, and (3) ensuring organization leadership continuity. | GAO-02-24, INFORMATION SHARING (3) |
| 12. | Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (3) |
| 13. | Among the challenges identified, one of the most difficult was overcoming new members' initial reluctance to share information. Other challenges included:<br>(1) developing agreements on the use and protection of shared information, (2) obtaining adequate funding to cover the cost of items such as Web sites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization, (3) maintaining a focus on emerging issues of interest to members, and (4) maintaining professional and administrative staff with appropriate skills | GAO-02-24, INFORMATION SHARING (4) |
| 14. | The Treasury CIP Program and other programs must be integrated into the underlying management philosophy of the Department and its subordinate units. | Treasury Critical Infrastructure Protection Plan (3) |
| 15. | The BCP and Test Reports will provide an organized and tested response to a major service interruption, document each Bureau's responsibilities for developing recovery policies and providing oversight of procedures, and accomplish the following primary objectives for supporting continuity planning:<br>Prioritize business processes across the Treasury<br>Ensure synchronization of information technology (IT) systems and business processes. | TCIP: Interdependency Analysis Methodology (5) |

| # | 6.1 Advisory Description | Source |
|---|---|---|
| | Match recovery capabilities to known business requirements.<br>Provide a coordinated response to potential disaster events.<br>Improve security functionality and survivability of assets.<br>Promote more efficient use of total resources.<br>Fulfill legislative mandates for protecting mission-essential assets and ensuring continuity of operations.<br>Methodically move the Treasury's security posture to an ideal state of mission assurance | |
| 16. | The Privacy Impact Assessment (PIA) describes the process used to guide system owners and developers in assessing privacy throughout all phases of the system development. All procedures that address the use, storage, retrieve-ability, accessibility, retention, and disposal of Privacy Act information are examined. One important aspect of the Privacy Act is to ensure that an accurate record of each disclosure of an individual's record and tax/financial data to any person or agency is maintained. The assessment requires the business system owner(s) and developer(s) to answer privacy-related questions. The PIA asks questions about the data in the system, access to the data, attributes of the data, and maintenance of administrative controls. | TCIP: Interdependency Analysis Methodology (7) |
| 17. | The CIO is responsible for providing guidance and direction to field personnel responsible for disaster recovery of off-premises storage activities. | IRM 25.10.1 (41) |
| 18. | Managers of the information technology services at IRS sites will coordinate the following with the appropriate business units:<br>a. acquisition of space for alternate processing facilities,<br>b. expeditious acquisition and transportation of replacement equipment required to restore operations,<br>c. development of processing priorities for completion of work following emergencies that degrade computer processing capabilities,<br>d. assessment of personnel requirements to support a distressed computer<br>e. processing operation to include occupation of an alternate processing facility, and<br>f. estimation of supplies and office equipment needed to support a computer processing operation occupying an alternate processing facility. | IRM 25.10.1 (44) |

## 6.2 Risk Evaluation and Control

### Table 3. Requirements for Risk Evaluation and Control

| # | 6.2 Requirement Description | Source |
|---|---|---|
| 1. | Identify systems containing sensitive information | Computer Security Act (5) |
| 2. | NIST Standards and Guides are compulsory and binding | Clinger/Cohen (7) |
| 3. | Critical Infrastructure defined | Patriot Act (4) |
| 4. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>…(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency; | FISMA (3) |
| 5. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency; | FISMA (8) |
| 6. | Any interruptions or manipulations of critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental | PDD-63 (3) |
| 7. | Agencies shall support the Public-Private Partnership to Reduce Vulnerability | PDD-63 (4) |
| 8. | Agencies shall conduct a vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure. | PDD-63 (10) |
| 9. | Homeland Security Advisory System shall be binding on the executive branch | HSPD-3 (2) |
| 10. | HSPD Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. | HSPD-3 (3) |
| 11. | All Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system | HSPD-3 (4) |
| 12. | Ensure that plans consider the consequences for essential services provided by State and local governments, and by the private sector, if the flow of Federal funds is disrupted | EO 12656 (8) |
| 13. | Ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities. | EO 12656 (9) |
| 14. | Assess essential emergency requirements and plan for the possible use of alternative resources to meet essential demands during and following national security emergencies | EO 12656 (11) |

| # | 6.2 Requirement Description | Source |
|---|---|---|
| 15. | Identify occupations and skills for which there may be a critical need in the event of a national security emergency. | EO 12656 (12) |
| 16. | Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency; | EO 12656 (14) |
| 17. | Develop plans to maintain stable economic conditions and a market economy during national security emergencies | EO 12656 (18) |
| 18. | Providing the Federal Government with efficient and equitable financing sources and payment mechanisms; | EO 12656 (19) |
| 19. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 20. | Each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. | 36CFR1220 (3) |
| 21. | Individual NCS member organizations will:<br>Identify their essential emergency functions (EEFs) and NSEP telecommunications needs and requirements | 47CFR216 (6) |
| 22. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 23. | A principle of Enterprise Architecture is to establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems. | OMB A-130 (8) |
| 24. | To support agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:<br>(i) Prioritize key systems (including those that are most critical to agency operations);<br>(ii) Apply OMB policies and, for non-national security applications, NIST guidance | OMB A-130 (9) |
| 25. | Agencies must use the National Institute of Standards and Technology (NIST) self-assessment guide to review their systems. | OMB-02-09 (7) |
| 26. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |

| # | 6.2 Requirement Description | Source |
|---|---|---|
| 27. | Agencies shall perform a risk analysis of their current operating facility and consider all possible scenarios that could require a COOP relocation | FEMA FPC-67 (4) |
| 28. | Scenarios should include small and large contingencies. | NIST SP 800-12 (4) |
| 29. | Identify preventive measures that deter, detect, or reduce impacts to the system. | NIST SP 800-34 (6) |
| 30. | Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing. | GAO-01-1168T, Critical Infrastructure Protection (8) |
| 31. | Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported by management and staff throughout the organization. | GAO-01-1168T, Critical Infrastructure Protection (2) |
| 32. | The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to:<br>Provide and maintain adequate levels of security for critical information systems, including emergency preparedness communications systems, for programs under its control. | Treasury Critical Infrastructure Protection Plan (5) |
| 33. | Each Head of Office shall:<br>b. utilize the results of the site's Risk Assessment to develop disaster scenarios and establish the basis for conducting a Business Impact Analysis (BIA); | IRM 25.10.1 (15) |
| 34. | The IRS cannot identify all events that may occur; however, those events that are most likely to happen must be identified, as well as the most cost effective controls to minimize the impact or eliminate the event from happening | IRM 25.10.1 (40) |

## Table 4. Advisories and Guides for Risk Evaluation and Control

| # | 6.2 Advisory Description | Source |
|---|---|---|
| 1. | Agencies may exceed NIST standards | Clinger/Cohen Act (8) |
| 2. | National Security System definition | Clinger/Cohen Act (10) |
| 3. | National Infrastructure Simulation and Analysis Center (NISAC) to serve as source of national competence for activities related to counter-terrorism, threat assessment, and risk mitigation. | Patriot Act (3) |
| 4. | Agencies shall strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack; | EO 13228 (8) |

| # | 6.2 Advisory Description | Source |
|---|---|---|
| 5. | Agencies shall develop criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities within the United States | EO 13228 (10) |
| 6. | The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices. The Director of OMB in this function and shall be reasonably cognizant of programs related to security of department and agency information systems. | EO 13231 (5) |
| 7. | Definition of “Records” | 36CFR1220 (2) |
| 8. | Vital Records Definitions | 36CFR1236 (4) |
| 9. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 10. | NSEP TSP [Telecommunications Service Priority] System allows the assignment of priority levels to any NSEP service across three time periods, or stress conditions: Peacetime/Crisis/Mobilization, Attack/War, and Post-Attack/Recovery. | 47CFR216 (9) |
| 11. | The NIST Risk Management guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. | NIST SP 800-30 (1) |
| 12. | The vital records and records disaster mitigation and recovery programs relate to emergency preparedness. | NARA Vital Records Guide (3) |
| 13. | The vital records program is intended to do two basic things. First, the program provides an agency with the information it needs to conduct its business under other than normal operating conditions and to resume normal business afterward. Second, the program enables agency officials to identify and protect the most important records dealing with the legal and financial rights both of the agency and of persons directly affected by the agency’s actions. | NARA Vital Records Guide (4) |
| 14. | Elements to consider when doing risk assessments:<br>Identifying threats that could harm and, thus, adversely affect critical operations and assets.<br>Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.<br>Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.<br>Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.<br>Identifying cost-effective actions to mitigate or reduce the risk.<br>Documenting the results and developing an action plan. | GAO-00-33, Information Security Risk Assessment (1) |

| # | 6.2 Advisory Description | Source |
|---|---|---|
| 15. | Access Controls. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and to keep records of individual user's actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and terminated employees and changes in users' responsibilities and related access needs. | GAO-00-295, INFORMATION SECURITY (3) |
| 16. | Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (7) |
| 17. | TCIPP establishes a systematic process the Department will use for identifying and analyzing critical infrastructure risks and making informed decisions regarding critical infrastructure safeguards. | Treasury Critical Infrastructure Protection Plan (4) |
| 18. | Offices and Bureaus shall:<br>Implement and maintain mitigation measures for their respective critical infrastructure. | Treasury Critical Infrastructure Protection Plan (15) |

## 6.3 Business Impact Analysis

### Table 5. Requirements for Business Impact Analysis

| # | 6.3 Requirement Description | Source |
|---|---|---|
| 1. | Identify systems containing sensitive information | Computer Security Act (5) |
| 2. | Minimize Critical Infrastructure disruptions | Patriot Act (2) |
| 3. | Critical Infrastructure Defined | Patriot Act (4) |
| 4. | Any interruptions or manipulations of critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental | PDD-63 (3) |
| 5. | Agencies shall conduct a vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure. | PDD-63 (10) |
| 6. | Homeland Security Advisory System shall be binding on the executive branch | HSPD-3 (2) |
| 7. | HSPD Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. | HSPD-3 (3) |
| 8. | All Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system | HSPD-3 (4) |
| 9. | Identify actions that could be taken in the early stages of a national security emergency or pending national security emergency to mitigate the impact of or reduce significantly the lead times associated with full emergency action implementation; | EO 12656 (7) |
| 10. | Ensure that plans consider the consequences for essential services provided by State and local governments, and by the private sector, if the flow of Federal funds is disrupted | EO 12656 (8) |
| 11. | Ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities. | EO 12656 (9) |
| 12. | Assess essential emergency requirements and plan for the possible use of alternative resources to meet essential demands during and following national security emergencies | EO 12656 (11) |
| 13. | Identify occupations and skills for which there may be a critical need in the event of a national security emergency. | EO 12656 (12) |
| 14. | Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency; | EO 12656 (14) |
| 15. | Develop plans to maintain stable economic conditions and a market economy during national security emergencies | EO 12656 (18) |

| # | 6.3 Requirement Description | Source |
|---|---|---|
| 16. | Providing the Federal Government with efficient and equitable financing sources and payment mechanisms; | EO 12656 (19) |
| 17. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 18. | Each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. | 36CFR1220 (3) |
| 19. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 20. | A principle of Enterprise Architecture is to establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems. | OMB A-130 (8) |
| 21. | To support agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:<br>(i) Prioritize key systems (including those that are most critical to agency operations);<br>(ii) Apply OMB policies and, for non-national security applications, NIST guidance | OMB A-130 (9) |
| 22. | For GISRA reporting, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. | OMB M-02-09 (5) |
| 23. | Agencies must use the National Institute of Standards and Technology (NIST) self-assessment guide to review their systems. | OMB-02-09 (7) |
| 24. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 25. | It is necessary not only to identify critical missions and businesses, but also to *set priorities for* them. A fully redundant capability for each function is prohibitively expensive for most organizations. | NIST SP 800-12 (2) |
| 26. | Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.  Resources that support critical functions:<br>Human Resources<br>Processing Capability | NIST SP 800-12 (3) |

| # | 6.3 Requirement Description | Source |
|---|---|---|
| | Computer-Based Services<br>Data and Applications<br>Physical Infrastructure<br>Documents and Papers | |
| 27. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions should be address:<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST SP 800-26 (3) |
| 28. | For the Business Impact Analysis, Agencies should<br>Identify Critical IT Resources<br>Identify Disruption Impacts and Allowable Outage Times<br>Develop Recovery Priorities | NIST SP 800-34 (5) |
| 29. | Service continuity controls ensure that, when unexpected events occur, critical operations continue without undue interruption and that critical and sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. | GAO-00-295, INFORMATION SECURITY (7) |
| 30. | Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location. | GAO-00-295, INFORMATION SECURITY (9) |
| 31. | To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. | GAO-01-1168T, Critical Infrastructure Protection (9) |
| 32. | … it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (4) |

| # | 6.3 Requirement Description | Source |
|---|---|---|
| 33. | Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (9) |
| 34. | During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations & Assets (10) |
| 35. | NARA's responsibilities stem from the Federal Records Act, which requires each federal agency to make and preserve records that (1) document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and (2) provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities. | GAO-02-586, INFORMATION MANAGEMENT: Challenges in Managing and Preserving Electronic Records (2) |
| 36. | First, agencies are required to maintain an inventory of all agency information systems. The inventory should identify (1) the system's name; (2) its purpose; (3) the agency programs supported by the system; (4) data inputs, sources, and outputs; (5) the information content of databases; and (6) the system's hardware and software environment. | GAO-02-586, INFORMATION MANAGEMENT: Challenges in Managing and Preserving Electronic Records (3) |
| 37. | The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to:<br>Integrate cost-effective security into government information systems that support national security and other essential government programs | Treasury Critical Infrastructure Protection Plan (7) |
| 38. | Offices and Bureaus shall:<br>Conduct business impact assessments for critical cyber and physical assets. | Treasury Critical Infrastructure Protection Plan (13) |
| 39. | Each Head of Office shall:<br>c. conduct a BIA to establish recovery priorities for business processes and their required information systems; | IRM 25.10.1 (16) |
| 40. | Each site, based on National business function objectives, will define their overall Business Processes and Mission Critical Application(s) MCA(s); this should include National PDD–63, Critical Assets, and recovery priorities. | IRM 25.10.1 (26) |
| 41. | Before any plan can be developed, research must be done in the overall strategy of business continuity and business resumption planning to ensure that all components of the operations have been clearly defined and prioritized in terms of criticality and the impact their loss would incur to the IRS. | IRM 25.10.1 (37) |
| 42. | An in-depth Business Impact Analysis (BIA) must be performed. This analysis must define the profile of critical business functions performed in all IRS functional areas IRS-wide. The IRS' facilities, geographical locations, sensitivity or criticality of information, and dependencies vary to such a degree that the effects of a disaster to one location will impact in a completely different manner for another. | IRM 25.10.1 (38) |

### Table 6. Advisories and Guides for Business Impact Analysis

| # | 6.3 Advisory Description | Source |
|---|---|---|
| 1. | National Security System definition | Clinger/Cohen Act (10) |
| 2. | Agencies shall strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack; | EO 13228 (8) |
| 3. | Definition of "Records" | 36CFR1220 (2) |
| 4. | Vital Records Definitions. | 36CFR1236 (4) |
| 5. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 6. | NSEP TSP [Telecommunications Service Priority] System allows the assignment of priority levels to any NSEP service across three time periods, or stress conditions: Peacetime/Crisis/Mobilization, Attack/War, and Post-Attack/Recovery. | 47CFR216 (9) |
| 7. | The vital records and records disaster mitigation and recovery programs relate to emergency preparedness. | NARA Vital Records Guide (3) |
| 8. | The vital records program is intended to do two basic things. First, the program provides an agency with the information it needs to conduct its business under other than normal operating conditions and to resume normal business afterward. Second, the program enables agency officials to identify and protect the most important records dealing with the legal and financial rights both of the agency and of persons directly affected by the agency's actions. | NARA Vital Records Guide (4) |
| 9. | The [Business Continuity Plan(s)] BCP for the Treasury and its Bureaus will address the survivability/continuity of critical business functions and set the stage for complete service restoration. The *BCP* will enable organized responses to emergency situations and identify risk mitigation strategies. The BCP typically incorporates the Occupant Emergency, Incident Management, Business Resumption, and Disaster Recovery Plans | TCIP: Interdependency Analysis Method (2) |

## 6.4 Business Continuity Strategies

### Table 7. Requirements for Business Continuity Strategies

| # | 6.4 Requirement Description | Source |
|---|---|---|
| 1. | NIST Standards and Guides are compulsory and binding | Clinger/Cohen Act (7) |
| 2. | Minimize Critical Infrastructure disruptions | Patriot Act (2) |
| 3. | Critical Infrastructure defined | Patriot Act (4) |
| 4. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate; | FISMA (5) |
| 5. | Any interruptions or manipulations of critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental | PDD-63 (3) |
| 6. | Agencies shall support the Public-Private Partnership to Reduce Vulnerability | PDD-63 (4) |
| 7. | Each Federal Agency is responsible for protecting its own critical infrastructure | PDD-63 (9) |
| 8. | Following an infrastructure attack, Agencies shall have a system to reconstitute minimum required capabilities rapidly. | PDD-63 (11) |
| 9. | Agencies shall develop Continuity of Operations Plans for Essential Operations | PDD-67 (3) |
| 10. | The assignment of an HSPD Threat Condition shall prompt the implementation of an appropriate set of Protective Measures | HSPD-3 (5) |
| 11. | Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. | HSPD-3 (6) |
| 12. | Identify actions that could be taken in the early stages of a national security emergency or pending national security emergency to mitigate the impact of or reduce significantly the lead times associated with full emergency action implementation; | EO 12656 (7) |
| 13. | Ensure that plans consider the consequences for essential services provided by State and local governments, and by the private sector, if the flow of Federal funds is disrupted | EO 12656 (8) |
| 14. | Ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities. | EO 12656 (9) |
| 15. | Assess essential emergency requirements and plan for the possible use of alternative resources to meet essential demands during and following national security emergencies | EO 12656 (11) |
| 16. | Identify occupations and skills for which there may be a critical need in the event of a national security emergency. | EO 12656 (12) |

| # | 6.4 Requirement Description | Source |
|---|---|---|
| 17. | Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency; | EO 12656 (14) |
| 18. | Develop plans to maintain stable economic conditions and a market economy during national security emergencies | EO 12656 (18) |
| 19. | Providing the Federal Government with efficient and equitable financing sources and payment mechanisms; | EO 12656 (19) |
| 20. | Agencies shall review and assess the adequacy of the portions of all Federal emergency response plans that pertain to terrorist threats or attacks within the United States; | EO 13228 (5) |
| 21. | Agencies shall identify programs that contribute to the Administration's strategy for homeland security and, in the development of the President's annual budget submission. The Office of Homeland Security shall review and provide advice to the heads of departments and agencies for such programs. | EO 13228 (18) |
| 22. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 23. | Each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. | 36CFR1220 (3) |
| 24. | Agencies shall ensure that the management of electronic records incorporates the following elements:<br>Specifying the location, manner, and media in which electronic records will be maintained; and<br>Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically. | 36CFR1234 (1) |
| 25. | Agencies shall implement and maintain an effective records security program that provides for backup and recovery of records to protect against information loss. | 36CFR1234 (2) |
| 26. | Agencies shall ensure that vital records and copies of vital records are adequately protected, accessible, and immediately usable. | 36CFR1236 (5) |
| 27. | Agencies shall take appropriate measures to ensure the survival of the vital records or copies of vital records in case of emergency or disaster. | 36CFR1236 (8) |
| 28. | [COG facilities design] Security design must support the continuity of Government operations during civil disturbances, natural disasters and other emergency situations. | 41CFR102-76 (2) |
| 29. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the | OMB A-130 (5) |

| # | 6.4 Requirement Description | Source |
|---|---|---|
| | loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | |
| 30. | A principle of Enterprise Architecture is to establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems. | OMB A-130 (8) |
| 31. | To support agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:<br>(i) Prioritize key systems (including those that are most critical to agency operations);<br>(ii) Apply OMB policies and, for non-national security applications, NIST guidance | OMB A-130 (9) |
| 32. | Investments in the development of new or the continued operation of existing information systems, must:<br>Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;<br>Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; | OMB A-130 (10) |
| 33. | Agency Security plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. | OMB A-130 (22) |
| 34. | For GISRA reporting, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. | OMB M-02-09 (5) |
| 35. | Agencies must use the National Institute of Standards and Technology (NIST) self-assessment guide to review their systems. | OMB-02-09 (7) |
| 36. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 37. | The Agency COOP plan should delineate essential functions and activities | FEMA FPC-65 (4) |
| 38. | All agencies should identify their essential functions as the basis for COOP planning. | FEMA FPC-65 (5) |
| 39. | Agencies are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are an essential part of an agency’s COOP plan. | FEMA FPC-65 (6) |
| 40. | Agencies shall designate alternate operating facilities as part of their COOP planning responsibilities. | FEMA FPC-67 (2) |
| 41. | Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business | NIST SP 800-18 (3) |

| # | 6.4 Requirement Description | Source |
|---|---|---|
| | interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. | |
| 42. | Contingency plans should be tested regularly to assure the continuity of support in the event of system failure | NIST SP 800-18 (5) |
| 43. | Contingency Plans describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable. Plans include descriptions for the following:<br>Any agreements of backup processing<br>Documented backup procedures<br>Location of stored backups and generations of backups | NIST SP 800-18 (6) |
| 44. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions should be address:<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST SP 800-26 (3) |
| 45. | Business Continuity Strategies should include:<br>Backup Methods<br>Alternate Sites<br>Equipment Replacement<br>Roles and Responsibilities<br>Cost Considerations | NIST SP 800-34 (7) |
| 46. | Service continuity controls ensure that, when unexpected events occur, critical operations continue without undue interruption and that critical and sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. | GAO-00-295, INFORMATION SECURITY (7) |
| 47. | Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location. | GAO-00-295, INFORMATION SECURITY (9) |
| 48. | Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and |

| # | 6.4 Requirement Description | Source |
|---|---|---|
| | | Assets (5) |
| 49. | The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to:<br>Integrate cost-effective security into government information systems that support national security and other essential government programs | Treasury Critical Infrastructure Protection Plan (7) |
| 50. | The National Security Officer (NSO) shall provide and maintain documentation of the communications network at off-premises locations sufficient to meet the requirements of the Business Continuity Program addressed in the IRM. | IRM 25.10.1 (5) |
| 51. | Security and Telecommunications personnel shall ensure timely maintenance of communications network documentation in suitable off-premises locations to meet the requirements of the Business Continuity Program of this manual. | IRM 25.10.1 (6) |

### Table 8. Advisories and Guides for Business Continuity Strategies

| # | 6.4 Advisory Description | Source |
|---|---|---|
| 1. | Agencies may exceed NIST standards | Clinger/Cohen Act (8) |
| 2. | National Security System definition | Clinger/Cohen Act (10) |
| 3. | The market provides are the first choice for addressing the problem of critical infrastructure protection | PDD-63 (5) |
| 4. | Privacy information will be handled accurately, confidentially and reliably | PDD-63 (6) |
| 5. | Agencies shall use FPC 65 for use in developing viable and executable contingency plans for the continuity of operations (COOP). | PDD-67 (4) |
| 6. | Emergency plans and programs, and an appropriate state of readiness, including organizational infrastructure, shall be developed as an integral part of the continuing activities | EO 12656 (4) |
| 7. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 8. | Agencies shall strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack; | EO 13228 (8) |
| 9. | Agencies shall coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack; | EO 13228 (9) |
| 10. | Definition of "Records" | 36CFR1220 (2) |
| 11. | Vital Records Definitions. | 36CFR1236 (4) |
| 12. | The National Communications Systems (NCS) shall coordinate | 47CFR216 (5) |

| # | 6.4 Advisory Description | Source |
|---|---|---|
| | the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | |
| 13. | NSEP TSP [Telecommunications Service Priority] System allows the assignment of priority levels to any NSEP service across three time periods, or stress conditions: Peacetime/Crisis/Mobilization, Attack/War, and Post-Attack/Recovery. | 47CFR216 (9) |
| 14. | Planning Considerations for COOP Alternate Sites.<br>Maximum use should be made of existing field infrastructures and consideration should be given to other options, such as telecommuting locations, work-at-home, virtual offices, and joint or shared facilities.<br>Construction. Since the alternate facility will be located at a sufficient distance from the affected facility and in an area reasonably free from other risks, no specific construction requirements are identified. At a minimum, the facility should be constructed such that it is not uniquely susceptible to natural disaster risk factors (e.g., earthquakes, tornadoes, hurricanes, floods, etc.).<br>Space. Sufficient space should be available for relocated staff; contiguous space is desirable, however, non-contiguous space might be acceptable if adequate communications are in place to ensure effective operations of the relocated organization.<br>Billeting. If the alternate facilities are located at a distance from the primary site, plans should be developed to address housing for emergency staff (e.g., billeting within facility, local motels).<br>Site Transportation. Transportation resource requirements, if any, should be met at the relocation sites (e.g., buses, automobiles).<br>Communications. Communications should be provided in sufficient quantity and mode/media to effectively interface with other organizational elements (e.g., regional offices), other departments and agencies, and other government and private sector organizations (including key operations centers) critical to the performance of organization mission essential functions. Secure/nonsecure communication requirements should be incorporated as required.<br>Security. Sufficient personnel should be designated to provide perimeter, access, and internal security functions as required by organization policy and operations.<br>Life Support. Most life support items should be available from external sources (e.g., food, water, medical services, sanitation, power); however, if not, they need to be contained in the facility in sufficient quantities for the anticipated duration of operations. In addition, items such as unique medical supplies, medical records and housekeeping supplies should be brought to the facility with the relocated personnel or maintained in the facility. | FEMA FPC-67 (5) |
| 15. | Contingency planning involves more than planning for a move offsite after a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in the | NIST SP 800-12 (1) |

| # | 6.4 Advisory Description | Source |
|---|---|---|
| | event of disruptions | |
| 16. | A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. | NIST SP 800-12 (5) |
| 17. | The [Business Continuity Plan(s)] BCP for the Treasury and its Bureaus will address the survivability/continuity of critical business functions and set the stage for complete service restoration. The BCP will enable organized responses to emergency situations and identify risk mitigation strategies. The BCP typically incorporates the Occupant Emergency, Incident Management, Business Resumption, and Disaster Recovery Plans | TCIP: Interdependency Analysis Method (2) |
| 18. | Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). | GAO-01-1168T, Critical Infrastructure Protection (11) |
| 19. | Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (7) |

## 6.5 Emergency Response and Operations

### Table 9. Requirements for Emergency Response and Operations

| # | 6.5 Requirement Description | Source |
|---|---|---|
| 1. | Privacy- Publish Systems of Records Notices | Privacy Act of 1974 (3) |
| 2. | Privacy – Protect Private Information | Privacy Act of 1974 (4) |
| 3. | Agencies shall support the Public-Private Partnership to Reduce Vulnerability | PDD-63 (4) |
| 4. | Each Federal Agency is responsible for protecting its own critical infrastructure | PDD-63 (9) |
| 5. | Agencies shall develop Continuity of Operations Plans for Essential Operations | PDD-67 (3) |
| 6. | The assignment of an HSPD Threat Condition shall prompt the implementation of an appropriate set of Protective Measures | HSPD-3 (5) |
| 7. | Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. | HSPD-3 (6) |
| 8. | HSPD Severe Condition (Red) requires increasing or redirecting personnel to address critical emergency needs; | HSPD-3 (11) |
| 9. | HSPD Severe Condition (Red) requires assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; | HSPD-3 (12) |
| 10. | Development of a system of emergency actions that defines alternatives, processes, and issues to be considered during various stages of national security emergencies; | EO 12656 (6) |
| 11. | Identify actions that could be taken in the early stages of a national security emergency or pending national security emergency to mitigate the impact of or reduce significantly the lead times associated with full emergency action implementation; | EO 12656 (7) |
| 12. | Ensure that plans consider the consequences for essential services provided by State and local governments, and by the private sector, if the flow of Federal funds is disrupted | EO 12656 (8) |
| 13. | Ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities. | EO 12656 (9) |
| 14. | Assess essential emergency requirements and plan for the possible use of alternative resources to meet essential demands during and following national security emergencies | EO 12656 (11) |
| 15. | Maintain a capability to assess promptly the effect of attack and other disruptions during national security emergencies. | EO 12656 (16) |
| 16. | Make available to the Office [of Homeland Security] all information relating to terrorist threats and activities within the United States. | EO 13228 (3) |
| 17. | Agencies shall review and assess the adequacy of the portions of | EO 13228 (5) |

| # | 6.5 Requirement Description | Source |
|---|---|---|
| | all Federal emergency response plans that pertain to terrorist threats or attacks within the United States; | |
| 18. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 19. | Agencies shall ensure that the management of electronic records incorporates the following elements:<br>Specifying the location, manner, and media in which electronic records will be maintained; and<br>Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically. | 36CFR1234 (1) |
| 20. | Vital records include emergency plans and related records. Only the most recent and complete source of the vital information needs to be treated as vital records. | 36CFR1236 (6) |
| 21. | Agencies shall ensure that retrieval procedures for vital records require only routine effort to locate needed information. Agencies also shall ensure that all equipment needed to read vital records or copies of vital records will be available in case of emergency or disaster. | 36CFR1236 (7) |
| 22. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 23. | Investments in the development of new or the continued operation of existing information systems, must:<br>Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;<br>Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; | OMB A-130 (10) |
| 24. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 25. | Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. | NIST SP 800-18 (3) |
| 26. | Contingency plans should be tested regularly to assure the continuity of support in the event of system failure | NIST SP 800-18 (5) |
| 27. | Contingency Plans describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable. | NIST SP 800-18 (6) |

| # | 6.5 Requirement Description | Source |
|---|---|---|
| | Plans include descriptions for the following:<br>Any agreements of backup processing<br>Documented backup procedures<br>Location of stored backups and generations of backups | |
| 28. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions should be address:<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST SP 800-26 (3) |
| 29. | Develop IT Contingency Plans | NIST SP 800-34 (10) |
| 30. | The Occupant Emergency Plan Designated Official (DO)<br>Coordinates with all tenants and develops an emergency plan.<br>Selects and trains Occupant Emergency Organization members.<br>Ensures that appropriate procedures are followed during emergencies.<br>Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility.<br>Initiates activities to prepare occupants for emergencies and inform them of response procedures. | GSA OEP Guide (7) |
| 31. | The Occupant Emergency Plan Administrative Officer (AO)<br>Assists the Occupant Emergency Coordinator<br>Records enacted emergency procedures.<br>Maintains organization records and updates them monthly.<br>Provides required administrative services (phones, faxes, radios, etc.) and prepares reports. | GSA OEP Guide (8) |
| 32. | The Occupant Emergency Plan Physical Security Specialist (PSS)<br>Works with the Occupant Emergency Coordinator.<br>Provides advice on security and law enforcement matters.<br>Serves as liaison with Federal and local law enforcement agencies | GSA OEP Guide (9) |
| 33. | Each Head of Office shall:<br>g. implement emergency response procedures appropriate to government laws, regulations, and directives; | IRM 25.10.1 (20) |
| 34. | An assessment must be made of containment actions to be taken at the onset of an emergency to provide greater safety for personnel while decreasing the chances for major damage to equipment and facilities. | IRM 25.10.1 (39) |
| 35. | All Business Continuity Plans for critical operations must include provisions for the appropriate level of security for both the damaged facility and any operational alternate processing facility. | IRM 25.10.1 (53) |

| # | 6.5 Requirement Description | Source |
|---|---|---|
| 36. | A management team will direct all recovery operations from a pre-determined primary and alternate Command Center. | IRM 25.10.1 (54) |

### Table 10. Advisories and Guides for Emergency Response and Operations

| # | 6.5 Advisory Description | Source |
|---|---|---|
| 1. | Agencies shall use FPC 65 for use in developing viable and executable contingency plans for the continuity of operations (COOP). | PDD-67 (4) |
| 2. | President's National Security Telecommunications Advisory Committee shall conduct reviews and assessments of the effectiveness of the implementation of PD/NSC – 53, National Security Telecommunications Policy. | EO 12382 (2) |
| 3. | Emergency plans and programs, and an appropriate state of readiness, including organizational infrastructure, shall be developed as an integral part of the continuing activities | EO 12656 (4) |
| 4. | Design preparedness measures to permit a rapid and effective transition from routine to emergency operations | EO 12656 (5) |
| 5. | Coordinate the development and implementation of plans for the operation and continuity of essential domestic emergency functions of the Federal Government during national security emergencies | EO 12656 (22) |
| 6. | [GSA will] Develop national security emergency plans and procedures for the operation, maintenance, and protection of federally owned and occupied buildings managed by the General Services Administration, and for the construction, alteration, and repair of such buildings; | EO 12656 (25) |
| 7. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 8. | Agencies shall coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack; | EO 13228 (9) |
| 9. | The Office of Homeland Security shall coordinate efforts to ensure rapid restoration of transportation systems, energy production, transmission, and distribution systems; telecommunications; other utilities; and other critical infrastructure facilities after disruption by a terrorist threat or attack; | EO 13228 (12) |
| 10. | The Office of Homeland Security shall coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack; | EO 13228 (13) |
| 11. | The Office of Homeland Security shall coordinate Federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families | EO 13228 (15) |
| 12. | The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National | EO 13228 (16) |

| # | 6.5 Advisory Description | Source |
|---|---|---|
| | Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership. | |
| 13. | Vital Records Definitions | 36CFR1236 (4) |
| 14. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 15. | For Occupant Emergency Plans: The designated official is the highest-ranking official in a Federal facility or another person agreed on by all tenant agencies. In the absence of the DO, they may designate an alternate official(s) to carry out the duties. | GSA OEP Guide (4) |
| 16. | The DO establishes, develops, applies, and maintains the plan. This person also establishes, assists in staffing, and trains the emergency organization that includes your agency's employees. | GSA OEP Guide (5) |
| 17. | The Command Center Team (CCT) directs all emergency operations from the building's Command Center (CC).<br>Special consideration must be made for rapid transportation of team members from their workstations to the CC and for quick notification of team members of an emergency. | GSA OEP Guide (6) |

## 6.6 Develop and Implement Business Continuity Plans

### Table 11. Requirements for Develop and Implement BC Plans

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 1. | Privacy- Publish Systems of Records Notices | Privacy Act of 1974 (3) |
| 2. | Privacy – Protect Private Information | Privacy Act of 1974 (4) |
| 3. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate; | FISMA (5) |
| 4. | Agencies shall support the Public-Private Partnership to Reduce Vulnerability | PDD-63 (4) |
| 5. | Cooperate and coordinate CIP planning with state and local governments and first responders | PDD-63 (8) |
| 6. | Each Federal Agency is responsible for protecting its own critical infrastructure | PDD-63 (9) |
| 7. | Agencies shall develop Continuity of Operations Plans for Essential Operations | PDD-67 (3) |
| 8. | The assignment of an HSPD Threat Condition shall prompt the implementation of an appropriate set of Protective Measures | HSPD-3 (5) |
| 9. | Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. | HSPD-3 (6) |
| 10. | HSPD Elevated Condition (Yellow) requires implementing, as appropriate, contingency and emergency response plans. | HSPD-3 (9) |
| 11. | HSPD High Condition (Orange) requires preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; | HSPD-3 (10) |
| 12. | HSPD Severe Condition (Red) requires increasing or redirecting personnel to address critical emergency needs; | HSPD-3 (11) |
| 13. | HSPD Severe Condition (Red) requires assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources; | HSPD-3 (12) |
| 14. | Ensure that plans consider the consequences for essential services provided by State and local governments, and by the private sector, if the flow of Federal funds is disrupted | EO 12656 (8) |
| 15. | Ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities. | EO 12656 (9) |
| 16. | Assess essential emergency requirements and plan for the possible use of alternative resources to meet essential demands during and following national security emergencies | EO 12656 (11) |

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 17. | Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency; | EO 12656 (14) |
| 18. | Develop plans to maintain stable economic conditions and a market economy during national security emergencies | EO 12656 (18) |
| 19. | Providing the Federal Government with efficient and equitable financing sources and payment mechanisms; | EO 12656 (19) |
| 20. | Develop plans for initiating tax changes, waiving regulations | EO 12656 (20) |
| 21. | Agencies shall review and assess the adequacy of the portions of all Federal emergency response plans that pertain to terrorist threats or attacks within the United States; | EO 13228 (5) |
| 22. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 23. | Agencies must ensure that they maintain adequate information about their records moved to an off-site records storage facility | 36CFR1220 (4) |
| 24. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 25. | To support agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:<br>(i) Prioritize key systems (including those that are most critical to agency operations);<br>(ii) Apply OMB policies and, for non-national security applications, NIST guidance | OMB A-130 (9) |
| 26. | Investments in the development of new or the continued operation of existing information systems, must:<br>Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;<br>Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; | OMB A-130 (10) |
| 27. | The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST) | OMB A-130 (15) |
| 28. | Security Plans will address Continuity of Support. | OMB A-130 (16) |
| 29. | Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. | OMB A-130 (18) |

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 30. | For GISRA reporting, identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.<br>Systems that have a contingency plan.<br>Systems for which contingency plans that have been tested in past year. | OMB M-02-09 (6) |
| 31. | Agencies must use the National Institute of Standards and Technology (NIST) self-assessment guide to review their systems. | OMB-02-09 (7) |
| 32. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 33. | COOP Alternate facilities should provide:<br>Immediate capability to perform essential functions under various threat conditions, including threats involving weapons of mass destruction;<br>Sufficient space and equipment to sustain the relocating organization.<br>Interoperable communications with all identified essential internal and external organizations, critical customers, and the public;<br>Reliable logistical support, services, and infrastructure systems, including water, electrical power, heating and air conditioning, etc.<br>Ability to sustain operations for a period of up to 30 days;<br>Consideration for the health, safety, and emotional well-being of relocated employees; and,<br>Appropriate physical security and access controls. | FEMA FPC-65 (7) |
| 34. | COOP plans should account for identification and protection of the vital records, systems, and data management software and equipment, to include classified or sensitive data as applicable, necessary to perform essential functions and activities, and to reconstitute normal agency operations after the emergency. | FEMA FPC-65 (8) |
| 35. | Agencies shall designate alternate operating facilities as part of their COOP planning responsibilities. | FEMA FPC-67 (2) |
| 36. | For contingency planning, make appropriate preparations, document the strategies, and train employees. Also establish contracts and agreements, | NIST SP 800-12 (6) |
| 37. | Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. | NIST SP 800-18 (3) |
| 38. | Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations | NIST SP 800-18 (4) |

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 39. | Contingency plans should be tested regularly to assure the continuity of support in the event of system failure | NIST SP 800-18 (5) |
| 40. | Contingency Plans describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable.<br>Plans include descriptions for the following:<br>Any agreements of backup processing<br>Documented backup procedures<br>Location of stored backups and generations of backups | NIST SP 800-18 (6) |
| 41. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions should be address:<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST SP 800-26 (3) |
| 42. | Contingency plans must be based on a clearly defined policy | NIST SP 800-34 (4) |
| 43. | Develop IT Contingency Plans | NIST SP 800-34 (10) |
| 44. | Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan itself should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process. | GAO-01-1168T, Critical Infrastructure Protection (10) |
| 45. | General Support System Security Plans shall include the following controls: establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. | IRM 25.10.1 (4) |
| 46. | The National Security Officer (NSO) shall provide and maintain documentation of the communications network at off-premises locations sufficient to meet the requirements of the Business Continuity Program addressed in the IRM. | IRM 25.10.1 (5) |
| 47. | Business Resumption Plans shall be developed, tested, implemented, and maintained for all essential IT systems. | IRM 25.10.1 (11) |

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 48. | Each Head of Office shall:<br>d. establish a roster of knowledgeable personnel to serve on recovery teams (i.e. management team, damage assessment team, operations team, restoration team); | IRM 25.10.1 (17) |
| 49. | Business Continuity Plans shall include at least the following:<br>a. a copy of the site's Occupant Emergency Plan (OEP);<br>b. recovery strategies and procedures for all MCA(s) and Business Processes;<br>c. procedures to restore, once the site has been returned to normal operations, all MCA(s) and Business Processes;<br>d. procedures to move critical workload or functions to other sites or Centers within the IRS;<br>e. procedures to notify National Headquarters Office, external customers, emergency/evacuation personnel, contract personnel, state and local authorities, and other support personnel which may be required to assist in the sites recovery;<br>f. procedures identifying responsibilities for ensuring that mission critical operations will continue if normal processing or data communications is interrupted for an unacceptable period; and<br>g. a designation of OFFICIAL USE ONLY on critical portions of the plan, to ensure that only those persons who have a need-to-know will have access to the critical elements of the plan. | IRM 25.10.1 (29) |
| 50. | Schedules for backup frequencies and rotation schedules must be established for critical files stored off-premises. | IRM 25.10.1 (30) |
| 51. | Each site shall develop, maintain, and test an Incident Management Plan. | IRM 25.10.1 (31) |
| 52. | All media must be properly stored and accounted for and a complete listing of the contents must be stored off-premises. | IRM 25.10.1 (32) |
| 53. | End-users shall develop business unit plans for resumption of all critical processes within the organization. | IRM 25.10.1 (34) |
| 54. | Business Continuity/Business Resumption planning shall include Emergency Response, and Recovery Operations. | IRM 25.10.1 (36) |
| 55. | Managers of the information technology services at IRS sites will:<br>a. establish backup frequencies and rotation schedules for critical files stored off-premises, other than those identified by National Headquarters, as stipulated in IRM 2.7.1, Information Technology Services (ITS)— Information Technology Services Operations/Inter-Centers.<br>b. ensure that all media is properly stored and accounted for and a complete listing of the contents is stored off-premises. This information must also be included in the site's disaster recovery plans. | IRM 25.10.1 (42) |
| 56. | The location of the off-premises storage facility will be far enough away from the computing facility, so as to not be affected by the same threat, but close enough to allow a quick response when time is critical. | IRM 25.10.1 (45) |

| # | 6.6 Requirement Description | Source |
|---|---|---|
| 57. | Store the items listed below at the off-premises storage facility:<br>Security Plan<br>Configuration Management Plan<br>Business Continuity Plan<br>DR/BR Plans<br>Risk Assessment Report<br>Security Features Users Guide<br>Certification and Accreditation<br>Trusted Facility Manual | IRM 25.10.1 (46) |
| 58. | Each information system facility must establish a method for off-premises storage, magnetic media control and procedures for an annual audit of all media stored off-premises. | IRM 25.10.1 (47) |
| 59. | Critical information systems must have adequate backup documentation and storage. | IRM 25.10.1 (48) |
| 60. | Business Continuity plans will provide methods for adjusting the use of computer and telecommunication hardware in order to continue operations, including the use of an alternate processing facility. | IRM 25.10.1 (49) |
| 61. | It will be the responsibility of all IRS Areas Disaster Recovery Coordinators/Analysts to document the distribution of the Business Continuity Plan. | IRM 25.10.1 (57) |

### Table 12. Advisories and Guides for Develop and Implement BC Plans

| # | 6.6 Advisory Description | Source |
|---|---|---|
| 1. | Privacy information will be handled accurately, confidentially and reliably | PDD-63 (6) |
| 2. | Agencies shall use FPC 65 for use in developing viable and executable contingency plans for the continuity of operations (COOP). | PDD-67 (4) |
| 3. | Emergency plans and programs, and an appropriate state of readiness, including organizational infrastructure, shall be developed as an integral part of the continuing activities | EO 12656 (4) |
| 4. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 5. | The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership. | EO 13228 (16) |
| 6. | Vital Records Definitions | 36CFR1236 (4) |

| # | 6.6 Advisory Description | Source |
|---|---|---|
| 7. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 8. | Planning Considerations for COOP Alternate Sites.<br>Maximum use should be made of existing field infrastructures and consideration should be given to other options, such as telecommuting locations, work-at-home, virtual offices, and joint or shared facilities.<br>Construction.  Since the alternate facility will be located at a sufficient distance from the affected facility and in an area reasonably free from other risks, no specific construction requirements are identified. At a minimum, the facility should be constructed such that it is not uniquely susceptible to natural disaster risk factors (e.g., earthquakes, tornadoes, hurricanes, floods, etc.).<br>Space.  Sufficient space should be available for relocated staff; contiguous space is desirable, however, non-contiguous space might be acceptable if adequate communications are in place to ensure effective operations of the relocated organization.<br>Billeting.  If the alternate facilities are located at a distance from the primary site, plans should be developed to address housing for emergency staff (e.g., billeting within facility, local motels).<br>Site Transportation.  Transportation resource requirements, if any, should be met at the relocation sites (e.g., buses, automobiles).<br>Communications.  Communications should be provided in sufficient quantity and mode/media to effectively interface with other organizational elements (e.g., regional offices), other departments and agencies, and other government and private sector organizations (including key operations centers) critical to the performance of organization mission essential functions. Secure/nonsecure communication requirements should be incorporated as required.<br>Security.  Sufficient personnel should be designated to provide perimeter, access, and internal security functions as required by organization policy and operations.<br>Life Support.  Most life support items should be available from external sources (e.g., food, water, medical services, sanitation, power); however, if not, they need to be contained in the facility in sufficient quantities for the anticipated duration of operations. In addition, items such as unique medical supplies, medical records and housekeeping supplies should be brought to the facility with the relocated personnel or maintained in the facility. | FEMA FPC-67 (5) |
| 9. | The System Security Plan (SSP) reflects related policies and covers all major systems and facilities and the plan(s) for major applications and general support systems for the following items:<br>Incident response capability.  The Treasury and its Bureaus have established and implemented formal security incident response mechanisms and have made system users aware of these | TCIP: Interdependency Analysis Methodology (6) |

| # | 6.6 Advisory Description | Source |
|---|---|---|
| | mechanisms and how to use them.<br>Contingency planning, testing, and documented updates. The Treasury and its Bureaus have developed and established plans that include policies and procedures to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disasters. The plans will be periodically tested and updated to reflect that the changes made to hardware, software, and operational readiness is current. | |
| 10. | Department of Treasury Security Manual TD P 71– 10 provides uniform policies and general procedures to be used by the bureaus to carry out their respective responsibilities in the areas of personnel, physical, telecommunications, IT systems security, and emergency preparedness. | IRM 25.10.1 (9) |
| 11. | Managers of the information technology services at IRS sites will coordinate the following with the appropriate business units:<br>a. acquisition of space for alternate processing facilities,<br>b. expeditious acquisition and transportation of replacement equipment required to restore operations,<br>c. development of processing priorities for completion of work following emergencies that degrade computer processing capabilities,<br>d. assessment of personnel requirements to support a distressed computer<br>e. processing operation to include occupation of an alternate processing facility, and<br>f. estimation of supplies and office equipment needed to support a computer processing operation occupying an alternate processing facility. | IRM 25.10.1 (44) |
| 12. | Personnel considerations are a critical part of any disaster recovery and business resumption planning effort. Personnel planning needs range from cross training employees and replacement of casualties to relocation to alternate processing facilities. | IRM 25.10.1 (50) |
| 13. | Planning for supplies and office equipment is a necessary part of the disaster recovery and business resumption planning process. | IRM 25.10.1 (51) |
| 14. | Consider transportation needs to move personnel, mail, supplies, and equipment, if an alternate processing facility is activated. Include recovery procedures for damage to direct support area(s), such as the mail room or loading dock that can create additional transportation needs. | IRM 25.10.1 (52) |

## 6.7 Awareness and Training Program

### Table 13. Requirements for Awareness and Training Program

| # | 6.7 Requirement Description | Source |
|---|---|---|
| 1. | Personnel using computer systems containing sensitive material need periodic training | Computer Security Act (4) |
| 2. | Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. | HSPD-3 (6) |
| 3. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(4) security awareness training | FISMA (6) |
| 4. | Participate in interagency activities to assess the relative importance of various facilities and resources to essential military and civilian needs and to integrate preparedness and response strategies and procedures; | EO 12656 (15) |
| 5. | Maintain a capability to assess promptly the effect of attack and other disruptions during national security emergencies. | EO 12656 (16) |
| 6. | Agencies shall coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training Federal, State, and local employees who would be called upon to respond to such a threat or attack; | EO 13228 (6) |
| 7. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 8. | Agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately addresses these mission areas. | EO 13231 (6) |
| 9. | Coordinate [Recruitment, Retention, and Training] programs to ensure that government employees with responsibilities for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, are adequately trained and evaluated | EO 13231 (12) |
| 10. | Agencies will train personnel in skills appropriate to management of information; | OMB A-130 (3) |

| # | 6.7 Requirement Description | Source |
|---|---|---|
| 11. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 12. | Investments in the development of new or the continued operation of existing information systems, must:<br>Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;<br>Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; | OMB A-130 (10) |
| 13. | Security Plans will address Continuity of Support. | OMB A-130 (16) |
| 14. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 15. | Agencies shall periodically test, train, and exercise their COOP plans individually and collectively. | FEMA FPC-66 (2) |
| 16. | Agencies should develop a COOP TT&E program that incorporates all levels of the agency, including headquarters, regions, and field locations. Funding for the program is the responsibility of each agency.<br>The TT&E program should include: policy, guidance, and standards; training courses and materials; exercises of varying types and scope designed to improve the overall organizational response capability to emergency situations; a multi-year TT&E schedule; and evaluation and remedial action programs. | FEMA FPC-66 (4) |
| 17. | Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. | NIST SP 800-18 (3) |
| 18. | Contingency plans should be tested regularly to assure the continuity of support in the event of system failure | NIST SP 800-18 (5) |
| 19. | Contingency Plans describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable.<br>Plans include descriptions for the following:<br>Any agreements of backup processing<br>Documented backup procedures<br>Location of stored backups and generations of backups | NIST SP 800-18 (6) |

| # | 6.7 Requirement Description | Source |
|---|---|---|
| 20. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions should be address:<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST SP 800-26 (3) |
| 21. | Plan Testing, Training, and Exercises | NIST SP 800-34 (8) |
| 22. | The Occupant Emergency Plan Designated Official (DO)<br>Coordinates with all tenants and develops an emergency plan.<br>Selects and trains Occupant Emergency Organization members.<br>Ensures that appropriate procedures are followed during emergencies.<br>Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility.<br>Initiates activities to prepare occupants for emergencies and inform them of response procedures. | GSA OEP Guide (7) |
| 23. | To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises. | GAO-00-295, INFORMATION SECURITY (8) |
| 24. | General Support System Security Plans shall include the following controls: establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. | IRM 25.10.1 (4) |
| 25. | Each Head of Office shall:<br>f. establish and periodically test the capability to perform the agency functions that significantly effect IRS programs, property, finances, information systems, and other systems; | IRM 25.10.1 (19) |

### Table 14. Advisories and Guides for Awareness and Training Program

| # | 6.7 Advisory Description | Source |
|---|---|---|
| 1. | Coordinate among the heads of Federal, State, and local agencies the planning, conduct, and evaluation of national security emergency exercises; | EO 12656 (23) |
| 2. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 3. | Vital Records Definitions | 36CFR1236 (4) |
| 4. | Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (7) |

## 6.8 Maintain and Exercise Business Continuity Plans

Table 15. Requirements for Maintain and Exercise BC Plans

| # | 6.8 Requirement Description | Source |
|---|---|---|
| 1. | Establish a plan for the security and privacy of each Federal computer system | Computer Security Act (6) |
| 2. | Ensure that the information security policies, procedures, and practices are adequate | Clinger/Cohen (4) |
| 3. | Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. | HSPD-3 (6) |
| 4. | Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. | HSPD-3 (7) |
| 5. | Each agency shall develop, document, and implement an agency wide information security program, …, that includes:<br>(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices | FISMA (7) |
| 6. | Participate in interagency activities to assess the relative importance of various facilities and resources to essential military and civilian needs and to integrate preparedness and response strategies and procedures; | EO 12656 (15) |
| 7. | Maintain a capability to assess promptly the effect of attack and other disruptions during national security emergencies. | EO 12656 (16) |
| 8. | Agencies shall coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training Federal, State, and local employees who would be called upon to respond to such a threat or attack; | EO 13228 (6) |
| 9. | Protect against disruption of the operation of information systems for critical infrastructure and ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. | EO 13231 (3) |
| 10. | Agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately addresses these mission areas. | EO 13231 (6) |
| 11. | Agencies shall ensure that vital records and copies of vital records are adequately protected, accessible, and immediately usable. | 36CFR1236 (5) |
| 12. | Vital records include emergency plans and related records. Only the most recent and complete source of the vital information | 36CFR1236 (6) |

| # | 6.8 Requirement Description | Source |
|---|---|---|
| | needs to be treated as vital records. | |
| 13. | Agencies shall ensure that retrieval procedures for vital records require only routine effort to locate needed information. Agencies also shall ensure that all equipment needed to read vital records or copies of vital records will be available in case of emergency or disaster. | 36CFR1236 (7) |
| 14. | Agencies must provide asset services [maintenance of facility] that maintain continuity of Government operations | 41CFR102-74 (3) |
| 15. | Agencies will protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information; | OMB A-130 (4) |
| 16. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 17. | Investments in the development of new or the continued operation of existing information systems, must:<br>Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;<br>Ensure that the handling of personal information is consistent with relevant government-wide and agency policies; | OMB A-130 (10) |
| 18. | Altered System of Records Report [SORN]:<br>When adding a new routine use, exemption, or otherwise significantly altering an existing system of records – at least 40 days before change to system takes place | OMB A-130 (12) |
| 19. | Security Plans will address Continuity of Support. | OMB A-130 (16) |
| 20. | Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support | OMB A-130 (20) |
| 21. | Perform an independent review or audit of the security controls in each application at least every three years. | OMB A-130 (21) |
| 22. | For GISRA reporting, identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.<br>Systems that have a contingency plan.<br>Systems for which contingency plans that have been tested in past year. | OMB M-02-09 (6) |
| 23. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 24. | Agencies shall periodically test, train, and exercise their COOP plans individually and collectively. | FEMA FPC-66 (2) |
| 25. | Agencies should develop a COOP TT&E program that | FEMA FPC-66 (4) |

| # | 6.8 Requirement Description | Source |
|---|---|---|
| | incorporates all levels of the agency, including headquarters, regions, and field locations. Funding for the program is the responsibility of each agency.<br>The TT&E program should include: policy, guidance, and standards; training courses and materials; exercises of varying types and scope designed to improve the overall organizational response capability to emergency situations; a multi-year TT&E schedule; and evaluation and remedial action programs. | |
| 26. | A contingency plan should be tested periodically.<br>Responsibility for keeping the contingency plan current should be specifically assigned. | NIST SP 800-12 (7) |
| 27. | Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. | NIST SP 800-18 (3) |
| 28. | Contingency plans should be tested regularly to assure the continuity of support in the event of system failure | NIST SP 800-18 (5) |
| 29. | Contingency Plans describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable.<br>Plans include descriptions for the following:<br>Any agreements of backup processing<br>Documented backup procedures<br>Location of stored backups and generations of backups | NIST SP 800-18 (6) |
| 30. | Plan Testing, Training, and Exercises | NIST SP 800-34 (8) |
| 31. | Plan Maintenance of contingency plans | NIST SP 800-34 (9) |
| 32. | The Occupant Emergency Plan Designated Official (DO)<br>Coordinates with all tenants and develops an emergency plan.<br>Selects and trains Occupant Emergency Organization members.<br>Ensures that appropriate procedures are followed during emergencies.<br>Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility.<br>Initiates activities to prepare occupants for emergencies and inform them of response procedures. | GSA OEP Guide (7) |
| 33. | This [contingency] plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and Assets (6) |
| 34. | Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred. | GAO-02-231T, Improvements Needed to Reduce Risk to Critical Federal Operations and |

| # | 6.8 Requirement Description | Source |
|---|---|---|
| | | Assets (8) |
| 35. | Second, NARA requires agencies to schedule the electronic records maintained in its systems. Agencies must either schedule those records under specific schedules, completed through submission and approval of Standard Form 115 (SF 115*)*, *Request for Records Disposition Authority*, or pursuant to a general records schedule. | GAO-02-586, INFORMATION MANAGEMENT: Challenges in Managing and Preserving Electronic Records (4) |
| 36. | Offices and Bureaus shall:<br>Update their respective COOP and COG plans on at least an annual basis to ensure that the policies and procedures adequately address new and existing critical assets. | Treasury Critical Infrastructure Protection Plan (12) |
| 37. | Offices and Bureaus shall:<br>Participate in Treasury-directed continuity of operations exercises. | Treasury Critical Infrastructure Protection Plan (14) |
| 38. | Offices and Bureaus shall:<br>Ensure Treasury has current and accurate business continuity information about how CIP assets are being protected. | Treasury Critical Infrastructure Protection Plan (16) |
| 39. | General Support System Security Plans shall include the following controls: establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. | IRM 25.10.1 (4) |
| 40. | The National Security Officer (NSO) shall provide and maintain documentation of the communications network at off-premises locations sufficient to meet the requirements of the Business Continuity Program addressed in the IRM. | IRM 25.10.1 (5) |
| 41. | Security and Telecommunications personnel shall ensure timely maintenance of communications network documentation in suitable off-premises locations to meet the requirements of the Business Continuity Program of this manual. | IRM 25.10.1 (6) |
| 42. | Department of Treasury Information System Life Cycle Manual TD P 4–01 provides guidelines for ensuring that contingency plans are developed for each mission critical system; those systems that significantly affect bureau programs, property, finances, and other resources. Each plan must be tested at a frequency commensurate with the risk and magnitude of loss or harm that could result from the disruption of systems operation. | IRM 25.10.1 (8) |
| 43. | Business Resumption Plans shall be developed, tested, implemented, and maintained for all essential IT systems. | IRM 25.10.1 (11) |
| 44. | Each Head of Office shall:<br>e. ensure that Performance Measures are followed for the planning, implementation, testing, review, and maintenance of Business Continuity Plans for all critical business functions; | IRM 25.10.1 (18) |
| 45. | Each Head of Office shall:<br>f. establish and periodically test the capability to perform the agency functions that significantly effect IRS programs, property, finances, information systems, and other systems; | IRM 25.10.1 (19) |
| 46. | Each Head of Office shall:<br>h. develop exercise plans that include an agenda of anticipated | IRM 25.10.1 (21) |

| # | 6.8 Requirement Description | Source |
|---|---|---|
| | accomplishments, a list of participants, methodology for proceeding, and requirements for vendors, alternate sites, and off-premises storage facilities. All subsequent exercises will follow the plans verbatim to determine if they are complete and correct, or need modification; | |
| 47. | Each Head of Office shall:<br>i. develop exercise plans in accordance with the American National Standards Institute (ANSI)/Institute of Electrical and Electronics<br>Engineers (IEEE) Standard Software Test Documentation 829. The test case is explained in IRM Exhibit 25.10.1–16 and the exercise plan<br>Format is provided in Exhibit 25.10.1–17; | IRM 25.10.1 (22) |
| 48. | Each Head of Office shall:<br>j. perform at least one exercise of the Business Continuity Plan each year. Exercises must include one business process and one IT system. Exercises will not be used to evaluate the plans on a pass or fail basis, but will serve as an opportunity to enhance the plans and improve organizational recovery readiness; | IRM 25.10.1 (23) |
| 49. | Each Head of Office shall:<br>k. ensure that only backup files retrieved from the off-premises storage site are used for the recovery exercises. Backup files will not be pre-positioned at the recovery site; and | IRM 25.10.1 (24) |
| 50. | Each Head of Office shall:<br>l. forward [to Treasury] within thirty (calendar) days of any exercise, a description of the events, results, problems encountered and recommended solutions to the Office of Security Evaluation and Oversight for review. Accomplish all modifications to the Business Continuity Plan in the same time frame. | IRM 25.10.1 (25) |
| 51. | Business Continuity Plans shall be comprehensive, reviewed quarterly, tested annually, and updated as needed, to provide for the reasonable restoration of operations. | IRM 25.10.1 (28) |
| 52. | Each site shall develop, maintain, and test an Incident Management Plan. | IRM 25.10.1 (31) |
| 53. | All media must be properly stored and accounted for and a complete listing of the contents must be stored off-premises. | IRM 25.10.1 (32) |
| 54. | Audits of all off-premises storage facilities must be conducted on an annual basis. | IRM 25.10.1 (33) |
| 55. | End-users shall review and update plans at least annually or whenever major processing environment changes occur (e.g., physical site, hardware, software, operating system, etc.). | IRM 25.10.1 (35) |
| 56. | It is the responsibility of each Head of Office to perform at least one exercise of the Business Continuity Plan each year. | IRM 25.10.1 (55) |
| 57. | Plan Maintenance requires an assessment of changes to the application/system operations and environment and the effect of those changes on the performance of the plan at the time of any disruption to normal business operations. | IRM 25.10.1 (56) |

### Table 16. Advisories and Guides for Maintain and Exercise BC Plans

| # | 6.8 Advisory Description | Source |
|---|---|---|
| 1. | Coordinate among the heads of Federal, State, and local agencies the planning, conduct, and evaluation of national security emergency exercises; | EO 12656 (23) |
| 2. | There shall be a national security emergency exercise program that shall be supported by the heads of all appropriate Federal departments and agencies. | EO 12656 (2) |
| 3. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 4. | Vital Records Definitions | 36CFR1236 (4) |
| 5. | The National Communications Systems (NCS) shall coordinate the planning for and provision of NSEP [National Security Emergency Preparedness] communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. | 47CFR216 (5) |
| 6. | Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.<br>Have the most critical and sensitive operations and their supporting computer resources been identified?<br>Has a comprehensive contingency plan been developed and documented?<br>Are tested contingency/ disaster recovery plans in place? | NIST 800-26 (3) |
| 7. | The BCP [Business Continuity Plans] and Test Reports will provide an organized and tested response to a major service interruption, document each Bureau's responsibilities for developing recovery policies and providing oversight of procedures, and accomplish the following primary objectives for supporting continuity planning:<br>Prioritize business processes across the Treasury<br>Ensure synchronization of information technology (IT) systems and business processes.<br>Match recovery capabilities to known business requirements.<br>Provide a coordinated response to potential disaster events.<br>Improve security functionality and survivability of assets.<br>Promote more efficient use of total resources.<br>Fulfill legislative mandates for protecting mission-essential assets and ensuring continuity of operations.<br>Methodically move the Treasury's security posture to an ideal state of mission assurance | TCIP: Interdependency Analysis Methodology (5) |

## 6.9 Public Relations and Crisis Coordination

Table 17. Requirements for Public Relations and Crisis Coordination

| # | 6.9 Requirement Description | Source |
|---|---|---|
| 1. | Agencies shall support the Public-Private Partnership to Reduce Vulnerability | PDD-63 (4) |
| 2. | Distribute the results of information assurance  endeavors | PDD-63 (7) |
| 3. | National Infrastructure Protection Center (NIPC) will be linked electronically to warning and operations centers | PDD-63 (13) |
| 4. | HSPD Elevated Condition (Yellow) requires coordinating emergency plans as appropriate with nearby jurisdictions; | HSPD-3 (8) |
| 5. | Agencies shall, to the extent permitted by law, provide the [National Security Telecommunications Advisory] Committee such information with respect to national security telecommunications matters as it may require for the purpose of carrying out its functions. | EO 12382 (3) |
| 6. | Participate in interagency activities to assess the relative importance of various facilities and resources to essential military and civilian needs and to integrate preparedness and response strategies and procedures; | EO 12656 (15) |
| 7. | Develop plans for initiating tax changes, waiving regulations | EO 12656 (20) |
| 8. | The implementation of this [CIP] policy shall include a voluntary public-private partnership, involving corporate and non-governmental organizations. | EO 13231 (3) |
| 9. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 10. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 11. | The Command Center Team (CCT) directs all emergency operations from the building's Command Center (CC).<br>Special consideration must be made for rapid transportation of team members from their workstations to the CC and for quick notification of team members of an emergency. | GSA OEP Guide (6) |
| 12. | The Occupant Emergency Plan Designated Official (DO)<br>Coordinates with all tenants and develops an emergency plan.<br>Selects and trains Occupant Emergency Organization members.<br>Ensures that appropriate procedures are followed during emergencies.<br>Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility. | GSA OEP Guide (7) |

| # | 6.9 Requirement Description | Source |
|---|---|---|
| | Initiates activities to prepare occupants for emergencies and inform them of response procedures. | |
| 13. | The Occupant Emergency Plan Administrative Officer (AO)<br>Assists the Occupant Emergency Coordinator<br>Records enacted emergency procedures.<br>Maintains organization records and updates them monthly.<br>Provides required administrative services (phones, faxes, radios, etc.) and prepares reports. | GSA OEP Guide (8) |
| 14. | The Occupant Emergency Plan Physical Security Specialist (PSS)<br>Works with the Occupant Emergency Coordinator.<br>Provides advice on security and law enforcement matters.<br>Serves as liaison with Federal and local law enforcement agencies | GSA OEP Guide (9) |
| 15. | The federal government's strategy for protecting the nation's critical computer-dependent infrastructure sectors includes efforts to establish information sharing and analysis centers (ISACs) within both the federal government and individual industry sectors. | GAO-02-24, INFORMATION SHARING (1) |

Table 18. Advisories and Guides for Public Relations and Crisis Coordination

| # | 6.9 Advisory Description | Source |
|---|---|---|
| 1. | NIST provides standards and guidelines for Federal computer systems | Computer Security Act (2) |
| 2. | President's National Security Telecommunications Advisory Committee shall conduct reviews and assessments of the effectiveness of the implementation of PD/NSC – 53, National Security Telecommunications Policy. | EO 12382 (2) |
| 3. | The functions of the [Homeland Security] Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. | EO 13228 (2) |
| 4. | The Office of Homeland Security shall coordinate national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate | EO 13228 (4) |
| 5. | The Office [of Homeland Security] shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate | EO 13228 (7) |
| 6. | Agencies shall coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack; | EO 13228 (9) |
| 7. | The Office of Homeland Security shall coordinate efforts to respond to and promote recovery from terrorist threats or attacks within the United States. In performing this function, the Office | EO 13228 (11) |

| # | 6.9 Advisory Description | Source |
|---|---|---|
| | shall work with Federal, State, and local agencies, and private entities, as appropriate | |
| 8. | The Office of Homeland Security shall coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack; | EO 13228 (13) |
| 9. | The Office of Homeland Security shall work with the National Economic Council to coordinate efforts to stabilize United States financial markets after a terrorist threat or attack and manage the immediate economic and financial consequences of the incident | EO 13228 (14) |
| 10. | The Office of Homeland Security shall coordinate Federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families | EO 13228 (15) |
| 11. | The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership. | EO 13228 (16) |
| 12. | The Office of Homeland Security shall coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses. | EO 13228 (17) |
| 13. | There shall be a senior executive branch board [CIPB] to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:<br>(b) protection of Federal departments' and agencies' critical infrastructure; | EO 13231 (4) |
| 14. | The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices. The Director of OMB in this function and shall be reasonably cognizant of programs related to security of department and agency information systems. | EO 13231 (5) |
| 15. | Agencies, coordinate outreach to and consultation with the private sector, including corporations that own, operate, develop, and equip information, telecommunications, transportation, energy, water, health care, and financial services, on protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems; | EO 13231 (8) |
| 16. | Agencies shall assist in the development of voluntary standards and best practices [for CIP] | EO 13231 (9) |
| 17. | The NIPC will advise departments and agencies on legislation relating to protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. | EO 13231 (13) |
| 18. | Agencies shall make all reasonable efforts to keep the [NIPC] Chair fully informed in a timely manner, and to the greatest extent | EO 13231 (14) |

| # | 6.9 Advisory Description | Source |
|---|---|---|
| | permitted by law, of all programs and issues within the purview of the Board. The Chair, in consultation with the Board, may propose policies and programs to appropriate officials to ensure the protection of the Nation's information systems for critical infrastructure | |
| 19. | Upon the request of the [National Infrastructure Advisory Council] Chair, the executive branch departments and agencies shall provide the Council with information and advice relating to its functions | EO 13231 (16) |
| 20. | Vital Records Definitions | 36CFR1236 (4) |
| 21. | All of the organizations identified trust as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships. | GAO-02-24, INFORMATION SHARING (2) |
| 22. | Among the challenges identified, one of the most difficult was overcoming new members' initial reluctance to share information. Other challenges included (1) developing agreements on the use and protection of shared information, (2) obtaining adequate funding to cover the cost of items such as Web sites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization,<br>(3) maintaining a focus on emerging issues of interest to members, and (4) maintaining professional and administrative staff with appropriate skills. | GAO-02-24, INFORMATION SHARING (4) |

## 6.10 Coordination with Public Authorities

**Table 19. Requirements for Coordination with Public Authorities**

| # | 6.10 Requirement Description | Source |
|---|---|---|
| 1. | Cooperate and coordinate CIP planning with state and local governments and first responders | PDD-63 (8) |
| 2. | Participate in interagency activities to assess the relative importance of various facilities and resources to essential military and civilian needs and to integrate preparedness and response strategies and procedures; | EO 12656 (15) |
| 3. | The implementation of this [CIP] policy shall include a voluntary public-private partnership, involving corporate and non-governmental organizations. | EO 13231 (3) |
| 4. | Agencies coordinate outreach on protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems to State and local governments, as well as communities and representatives from academia and other relevant elements of society. | EO 13231 (8) |
| 5. | Consult with potentially affected communities, including the legal, auditing, financial, and insurance communities, to the extent permitted by law, to determine areas of mutual concern [for CIP] | EO 13231 (10) |
| 6. | Outreach on critical infrastructure protection issues with private sector organizations within the areas of concern to these departments and agencies | EO 13231 (11) |
| 7. | Agencies will ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information; Limit the collection of information which identifies individuals; Limit the sharing of information that identifies individuals or contains proprietary information; | OMB A-130 (5) |
| 8. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 9. | Agencies shall have in place a viable COOP capability [that] ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. | FEMA FPC-65 (2) |
| 10. | The Occupant Emergency Plan Designated Official (DO)<br>Coordinates with all tenants and develops an emergency plan.<br>Selects and trains Occupant Emergency Organization members.<br>Ensures that appropriate procedures are followed during emergencies.<br>Identifies and establishes working relationships with Federal, State, and local agencies that might respond to an emergency in the facility.<br>Initiates activities to prepare occupants for emergencies and inform them of response procedures. | GSA OEP Guide (7) |

| # | 6.10 Requirement Description | Source |
|---|---|---|
| 11. | The federal government's strategy for protecting the nation's critical computer-dependent infrastructure sectors includes efforts to establish information sharing and analysis centers (ISACs) within both the federal government and individual industry sectors. | GAO-02-24, INFORMATION SHARING (1) |

### Table 20. Advisories and Guides for Coordination with Public Authorities

| # | 6.10 Advisory Description | Source |
|---|---|---|
| 1. | Agencies shall coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack; | EO 13228 (9) |
| 2. | The Office of Homeland Security shall coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack; | EO 13228 (13) |
| 3. | The Office of Homeland Security shall work with the National Economic Council to coordinate efforts to stabilize United States financial markets after a terrorist threat or attack and manage the immediate economic and financial consequences of the incident | EO 13228 (14) |
| 4. | The Office of Homeland Security shall coordinate Federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families | EO 13228 (15) |
| 5. | The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership. | EO 13228 (16) |
| 6. | The Office of Homeland Security shall coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses. | EO 13228 (17) |
| 7. | Vital Records Definitions | 36CFR1236 (4) |
| 8. | The federal government's strategy for protecting the nation's critical computer-dependent infrastructure sectors includes efforts to establish information sharing and analysis centers (ISACs) within both the federal government and individual industry sectors. | GAO-02-24, INFORMATION SHARING (1) |
| 9. | Among the challenges identified, one of the most difficult was overcoming new members' initial reluctance to share information. Other challenges included (1) developing agreements on the use and protection of shared information, (2) obtaining adequate funding to cover the cost of items such as Web sites and meetings while avoiding seeking contributions intended primarily to promote the interests of an individual organization,<br>(3) maintaining a focus on emerging issues of interest to members, and (4) maintaining professional and administrative staff with appropriate skills. | GAO-02-24, INFORMATION SHARING (4) |

# Acronyms

| | |
|---|---|
| **AO** | Administrative Officer (OEP) |
| **BC** | Business Continuity |
| **BCI** | Business Continuity Institute |
| **BCM** | Business Continuity Management |
| **BCP** | Business Continuity Planning, Business Continuity Plan, Business Continuity Professional |
| **BCP&M** | Business Continuity Planning and Management |
| **BIA** | Business Impact Analysis |
| **BOD** | Business Operating Division |
| **BRP** | Business Resumption Plan |
| **CCT** | Command Center Team (OEP) |
| **CERT** | Computer Emergency Response Team |
| **CFR** | Code of Federal Regulations |
| **CIAO** | Critical Infrastructure Assurance Office/Officer |
| **CIO** | Chief Information Officer |
| **CIP** | Critical Infrastructure Protection |
| **CMC** | Crisis Management Center |
| **COG** | Continuity of Government |
| **COOP** | Continuity of Operations |
| **DO** | Designated Official (OEP) |
| **DR** | Disaster Recovery |
| **DRI, DRII** | Disaster Recovery Institute, International |
| **DRP** | Disaster Recovery Plan |
| **EA** | Enterprise Architecture |
| **EO** | Executive Order |
| **FEMA** | Federal Emergency Management Administration |
| **FISMA** | Federal Information Systems Management Act (of 2002) |
| **FMR** | Federal Management Regulations |
| **FOD** | Functional Operating Division |
| **FPC** | Federal Preparedness Circular |

| | |
|---|---|
| **GAO** | General Accounting Office |
| **GSA** | General Services Administration |
| **ICS** | Incident Command Structure |
| **IMP** | Incident Management Plan |
| **IRM** | Internal Revenue Manual |
| **IT** | Information Technology |
| **LOU** | Limited Official Use |
| **NARA** | National Archives and Records Administration |
| **nCIAO** | National Critical Infrastructure Assurance Office |
| **NIPC** | National Infrastructure Protection Center |
| **NIST** | National Institute of Standards and Technology |
| **OEP** | Occupancy Emergency Plan, Occupant Emergency Program |
| **OHS** | Office of Homeland Security |
| **OMB** | Office of Management and Budget |
| **PD(D)** | Presidential Decision (Directive) |
| **PL** | Public Law |
| **POD** | Post of Duty |
| **RPO** | Recovery Point Objective |
| **RTO** | Recovery Time Objective |
| **SAMC** | Situation Awareness and Management Center |
| **SCR/CR** | Senior Commissioner’s Representative or the Commissioner’s Representative |
| **SORN** | System of Records Notice |
| **TD** | Treasury Directive |
| **TIGTA** | Treasury Inspector General for Tax Administration |
| **USC** | United States Code |

# Glossary

**Alternate Recovery Site**
Sites at which work may be done if an incident renders a primary work site uninhabitable. This may be for short-term or long-term recovery.

**Business Continuity Management (BCM)**
Business Continuity Management is the process and procedures established by an organization that ensures that its business continuity plans are constantly up-to-date, its staff is trained, ready and able to execute the plans, and new developments support the organization's ability to quickly recover from any disruption of service.

**Business Continuity Plan (BCP)**
An all-encompassing, "umbrella" term covering occupant emergency planning, incident management planning, business resumption planning and, disaster recovery planning.

**Business Impact Analysis (BIA)**
The process of determining the impact on an organization should a potential loss identified by the risk analysis actually occurs. The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint.

**Business Resumption Plan (BRP)**
This is the complete plan, which is in reality a collection of plans. The collection has one plan that manages the incident called the Incident Management Plan. There is one functional Management Recovery Plan for EACH business function located at the site, and numerous Work Group Recovery Plans. This also may be referred to as a District Business Recovery Plan or a Comprehensive Business Recovery Plan.

**Continuity of Government (COG)**
The purpose of Enduring Constitutional Government (ECG), Continuity of Government (COG), and Continuity of Operations (COOP) is to ensure survival of a constitutional form of government and the continuity of essential Federal functions.

**Continuity of Operations (COOP)**
The purpose of Enduring Constitutional Government (ECG), Continuity of Government (COG), and Continuity of Operations (COOP) is to ensure survival of a constitutional form of government and the continuity of essential Federal functions.

**Critical Infrastructure**
Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

**Critical Infrastructure Protection (CIP)**
Critical Infrastructure Protection (CIP) is the ability to protect critical infrastructures.

**Critical Records**

Any information resources (paper or electronic) that is essential to conducting the IRS business. Vital records shall include:

A. Emergency Operating Records (e.g. delegations of authority, building plans, equipment inventories, system documentation); and

B. Rights and Interest Records (e.g. payroll, retirement, insurance, social security, accounts receivable records, etc.). When listing vital records, consider those records or documentation which, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or re-creation at considerable expense.

**Continuity of Operations**

Continuity of operations (COOP). COOP planning facilitates the performance of department/agency essential functions during any emergency or situation that may disrupt normal operations.

**Disaster**

This is an unplanned event that creates the inability of the organization to perform critical business functions for a predetermined period of time.

**Disaster Recovery (DR)**

Activities and programs designed to return the entity to an acceptable condition. [DRI]

The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions. [Disaster Recovery Journal]

A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [NIST]

**Disaster Recovery Plan (DRP)**

As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [NIST]

**Incident Command System (ICS)**

This is an established management functional and organizational hierarchy that is implemented to respond to the incident. It is the responsibility of the Incident Manager and the Head of Office to ensure the necessary parties are assigned to the needed ICS roles.

**Incident Management Plan (IMP)** This is the plan that provides for the overall coordination to manage the incident. The Incident Management Team and their support teams use this plan.

**Occupant Emergency Plan (OEP)** First level of emergency procedures to follow in the event of an incident ensuring the facility is evacuated timely. These procedures are generally developed by the facility and may be activated following an evacuation of the building when accessibility back to the facility will be delayed.

**Vital Records** Files determined by a Business Unit to be necessary to the restoration of their critical and essential functions. These files may be different from the Critical Records, in that these file are from a business restoration perspective only.

# List of References

1. Code of Federal Regulations, 29 CFR 1910.120, Hazardous waste operations and emergency response.

2. Code of Federal Regulations, 36 CFR 1236, Management of Vital Records, May 16, 2001

3. Code of Federal Regulations, 36 CFR 1220 Records Management, May 16, 2001

4. Code of Federal Regulations, 36 CFR 1234, Electronic Records Management, May 16, 2001

5. Code of Federal Regulations, 41 CFR 101-20.103.4, Management of Buildings and Grounds/Occupant Emergency Program

6. Code of Federal Regulations, 41 CFR 102-74, Continuity of Government Facilities

7. Code of Federal Regulations, 41 CFR 102-76, Continuity of Government Facilities Design

8. Code of Federal Regulations, 44 CFR 206, Disaster Declaration [No applicable BCP requirements identified.]

9. Code of Federal Regulations, 47 CFR 216, National Security Emergency Preparedness, October 1, 2001

10. Commercial: Andy Hagg, “Benchmark Report: BCP in 2002,” July 2002

11. Commercial: Business Continuity Institute (BCI), Continuity Planning – Contractual Issues, September 2002

12. Commercial: CERT Coordination Center, Survivable Systems Analysis Method, June 2002

13. Commercial: David Berlind, “Not Much New in Business Continuity. Not Even Budgets,” October 8, 2002

14. Commercial: David Davies, “Looking Back for The Future,” May 3, 20002

15. Commercial: David Honour, “Project Initiation and Management,” August 15, 2002

16. Commercial: EMC White Paper, “A Symmetrix White Paper: Disaster Recovery as Business Continuity,” June 2002

17. Commercial: Gary Leather, “Wider Than IT,” September 4, 2002

18. Commercial: Globalcontinuity.com, “Business Continuity Planning Practices Explored,” August 30, 2002

19. Commercial: Globalcontinuity.com, “Invocation Survey—Final Results,” July 17, 2002

20. Commercial: Globalcontinuity.com, “US Financial Institutions Face Tough New Business Continuity Regulations,” September 3, 2002

21. Commercial: John Fontana and Deni Connor, “Disaster Recovery Then and Now,” November 26, 2001

22. Commercial: Peter Power, “Disasters—Plan for Your People,” August 30, 2002

23. Commercial: Strohl Systems Online Newsroom Press Release, “Survey: More Than One Third of Organizations Have Activated Their Business Continuity Plans,” August 16, 2002

24. Commercial: Strohl Systems Online Newsroom Press Release, “Three Out Of Four Organizations Have Reviewed Their Business Continuity Plan Since Sept. 11,” February 7, 2002

25. Commercial: Victoria Hardy, “High-Profile Evacuation,” November 1, 2002

26. Commercial: Virtual Corporation, *Business Continuity Maturity Model*, September 4, 2002

27. Disaster Recovery Institute, International, *The Professional Practices for Business Continuity Planners,* May 2002

28. Executive Order 11490, Assigning Emergency Preparedness Functions to Federal Departments and Agencies, October 28, 1969 [No applicable BCP requirements identified.]

29. Executive Order 12241, National Contingency Plan, September 29, 1980 [No applicable BCP requirements identified, applies to environmental protection only.]

30. Executive Order 12382, President’s National Security Telecommunications Advisory Committee, September 13, 1982

31. Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984 [No applicable BCP requirements identified.]

32. Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 18, 1988 [amended by EO13228].

33. Executive Order 12958, Classified National Security Information, April 17, 1995 [No applicable BCP requirements identified.]

34. Executive Order 13010, Critical Infrastructure Protection, July 15, 1996 [Expired 1997]

35. Executive Order 13041, Further Amendment to Executive Order 13010, As Amended, April 3, 1997 [No applicable BCP requirements identified.]

36. Executive Order 13064, Further Amendment to Executive Order 13010, As Amended, Critical Infrastructure Protection, October 11, 1997 [No applicable BCP requirements identified.]

37. Executive Order 13138, Continuance of Certain Federal Advisory Committees, September 30, 1999 [No applicable BCP requirements identified.]

38. Executive Order 13225, Continuance of Certain Federal Advisory Committees, September 28, 2001 [No applicable BCP requirements identified.]

39. Executive Order 13226, President's Council of Advisors on Science and Technology, September 30, 2001 [No applicable BCP requirements identified.]

40. Executive Order 13228, Establishing Office of Homeland Security and the Homeland Security Council, October 8, 2001

41. Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001

42. Executive Order 13246, Providing an Order of Succession within the Department of Treasury, December 18, 2001 [No applicable IRS BCP requirements identified.]

43. Executive Order 13260, Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security, March 19, 2002

44. Federal Reserve, Board of Governors, et al, *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial Systems*, August 30, 2002

45. FEMA 9230.1, Federal Response Plan, April 1999

46. FEMA FPC 65, Federal Executive Branch Continuity of Operations, July 26, 1999

47. FEMA FPC 66, Test Training and Exercise (TT&E) for Continuity of Operations, April 30, 2001

48. FEMA FPC 67, Acquisition of Alternate Facilities for Continuity of Operations, April 30, 2001

49. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO-00-295, September 2000

50. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO-00-33, November 1999

51. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks*, GAO-01-1168T, September 26, 2001

52. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24, October 2001

53. General Accounting Office, *Information Management: Challenges in Managing and Preserving Electronic Records*, GAO-02-586, October 2001

54. GSA, Public Building Service, Federal Protective Service – Occupant Emergency Program Guide, March 2002

55. National Archives and Records Administration, *Vital Records and Records Disaster Mitigation and Recovery, An Instructional Guide*, 1999 Web Edition

56. National Institutes of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication (SP) 800–12, October 1995

57. NIST SP 800-14, *Contingency Planning Guide for Information Technology Systems*, September 1996

58. NIST SP 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996 [No applicable BCP requirements identified.]

59. NIST SP 800–18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998

60. NIST SP 800–23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Testes/Evaluated Products*, August 1999

61. NIST SP 800–26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001

62. NIST SP 800–27, *Engineering Principles for Information Technology Security*, June 2001 [No applicable BCP requirements identified.]

63. NIST SP 800–30, *Risk Management Guide for Information Technology Systems*, October 2001 [No applicable BCP requirements identified, but could be useful doing Risk Evaluations.]

64. NIST SP 800–34, *Contingency Planning Guide for Information Technology Systems*, June 2002

65. NIST SP 800–47, *Security Guide for Interconnecting Information Technology Systems*, October 2002 [No applicable BCP requirements identified.]

66. NIST SP 800–50, *Building an Information Technology Security Awareness and Training Program*, 1st Draft, July 2002 [No applicable BCP requirements identified but could be useful setting up an awareness and training program.]

67. Office of Management and Budget (OMB), Circular A–130, *Management of Federal Information Resources*, Transmittal 4, December 12, 2000

68. OMB Memorandum 01-08, “Guidance on Implementing Government Information Security Reform Act,” October 9, 2002 [No applicable BCP requirements identified.]

69. OMB Memorandum 02-01, “Guidance for Preparing and Submitting Security Plans of Action and Milestones,” October 17, 2001 [No applicable BCP requirements identified.]

70. OMB Memorandum 02-09, **“**Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones,” July 2, 2002

71. Public Law 100-235, Computer Security Act [of 1987]

72. Public Law 104-106, Information Technology Management Reform Act [Clinger/Cohen Act] February 10, 1996

73. Public Law 106-398, National Defense Authorization Fiscal Year 2001, Subtitle G – Government Information Security Reform, Sections 1061 – 1065

74. Public Law 106-56, Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act Of 2001), October 26, 2001

75. Public Law 107-347, E-Government Act of 2002, Title III Information Security, Federal Information Security Management Act [FISMA] of 2002, December 22, 2002.

76. Public Law, Privacy Act of 1974 [5 USC 552a]

77. Treasury Inspector General for Tax Administration (TIGTA) 2000-20-031: The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans, March 2000 [Limited Official Use Document – MITRE review in separate report]

78. TIGTA 2000-20-039: The Internal Revenue Service Can Improve Information Systems Physical Security, February 2000 [Limited Official Use Document – MITRE review in separate report]

79. TIGTA 2000-20-072: The General Controls Over a Critical Internal Revenue Service Tax Processing Computer System Can Be Strengthened, May 2000 [Limited Official Use Document – MITRE review in separate report]

80. TIGTA 2001-20-020: Computer Security Controls Should Be Strengthened in the Former Brooklyn District, November 2000 [Limited Official Use Document – MITRE review in separate report]

81. TIGTA 2001-20-036: Computer Security Controls Should Be Strengthened in the Former Northern California District, January 2001 [Limited Official Use Document – MITRE review in separate report]

82. TIGTA 2001-20-072: Disaster Recovery Plans for Mainframe Systems at the Tennessee Computing Center Have Improved, But Mid-Range Systems Still Need Attention, April 2001 [Limited Official Use Document – MITRE review in separate report]]

83. TIGTA 2001-20-092: Controls Over The IRS' Masterfile System Are Generally Adequate, But Some Improvement Is Needed, June 2001 [Limited Official Use Document – MITRE review in separate report]

84. TIGTA 2001-20-108: Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources, July 2001 [Limited Official Use Document – MITRE review in separate report]

85. TIGTA 2002-20-007: The Internal Revenue Service Encrypts Data Transmitted Between Its Facilities, But Controls Over Cryptography Can Be Improved, October 2001 [Limited Official Use Document – MITRE review in separate report]

86. TIGTA 2002-20-044: The System-Level Controls Over the Security and Communications System Are Adequate; However, Improvements Can Be Made, January 2002 [Limited Official Use Document – MITRE review in separate report]

87. TIGTA 2002-20-045: Controls Over the Procurement Web Site Should Be Improved to Better Deter and Detect External Attacks, January 2002 [Limited Official Use Document – MITRE review in separate report]

88. TIGTA 2002-20-057: Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems, March 2002 [Limited Official Use Document – MITRE review in separate report]

89. TIGTA 2002-20-064: Controls Over the Excise Files Information Retrieval System Web Site Should Be Improved to Better Deter and Detect External Attacks, April 2002 [Limited Official Use Document – MITRE review in separate report]

90. TIGTA 2002-20-082: System-Level Controls Over the Detroit Computing Center Mainframe Computers Are Generally Adequate, But Some Improvement Is Needed, April 2002 [Limited Official Use Document – MITRE review in separate report]

91. TIGTA 2002-30-054: The Centralization of Business Tax Return Processing to Two Submission Processing Centers Is on Schedule, but Disaster Contingency Plans Must Be Updated and Tested, February 2002 [Limited Official Use Document – MITRE review in separate report]

92. TIGTA 2003-20-026: The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program, but Continued Efforts Are Needed, December 2002 [MITRE review in separate report]

93. Treasury Critical Infrastructure Protection Plan (TCIPP), Version 2, Department of the Treasury, August 30, 2002

94. Treasury Critical Infrastructure Protection: Interdependency Analysis Method, Version 1.1, September 24, 2002

95. Treasury Directive 71-10, Department of Treasury Security Manual, August 23, 1999