

Appendix B. Department of the Treasury Business Continuity Requirements and Guides

This appendix contains the detailed reviews of the Department of the Treasury Directives and Treasury's plans. The applicable statements are captured in the following tables along with MITRE's assessment of whether the statement is a Requirement (R) that must be addressed, or Advice (A) that should be considered, or just a Comment (C) to put the information into context.

Table of Contents: Appendix B

B.1	Treasury Directives	3
B.1.1	71-10 – Department of Treasury Security Manual	3
B.2	Treasury CIP Plans	4
B.2.1	Department of Treasury Critical Infrastructure Protection Plan (TCIPP)	4
B.2.2	Treasury Critical Infrastructure Protection: Interdependency Analysis Method	7

B.1 Treasury Directives

The following Public Laws and their associated Acts have been determined to have requirements or advice that directly applies to specific areas under Business Continuity.

B.1.1 71-10 – Department of Treasury Security Manual

Ref #	Treasury Directive 71-10 Department of Treasury Security Manual, August 23, 1999	Applicable BC Process	Applicable BC Plans	Statement Class
1.	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).	1. Project Initiation & Management	BCM	R

Statement Class

A – Advice

C - Comment

R – Requirement

B.2 Treasury CIP Plans

This section contains detailed review of the plans produced of the Treasury Critical Infrastructure Protection Working Group products.

B.2.1 Department of Treasury Critical Infrastructure Protection Plan (TCIPP)

Ref #	Treasury Critical Infrastructure Protection Plan, Version 2, August 30, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
1.	Treasury Critical Infrastructure Protection Plan (TCIPP) describes the Treasury Department's strategy for protecting Treasury-owned and operated critical infrastructure that supports its key economic, financial, law enforcement, and management missions.			C
2.	The TCIPP responds to federal CIP guidance from Presidential Directives, Executive Orders (EO), and the Office of Management and Budget (OMB), and legislation. It also responds to the findings of the Final Audit Report: Review of Treasury's Critical Infrastructure Program, OIG-01-25, December 14, 2000.			C
3.	The Treasury CIP Program and other programs must be integrated into the underlying management philosophy of the Department and its subordinate units.	1. Project Initiation & Management	BCM, CIP	A
4.	TCIPP establishes a systematic process the Department will use for identifying and analyzing critical infrastructure risks and making informed decisions regarding critical infrastructure safeguards.	2. Risk Evaluation & Control	BCM	A
5.	The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to: <ul style="list-style-type: none"> • Provide and maintain adequate levels of security for critical information systems, including emergency preparedness communications systems, for programs under its control. 	2. Risk Evaluation & Control	BCM, CIP	R
6.	The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to: <ul style="list-style-type: none"> • Ensure development, and within available appropriations, fund programs that adequately address these [CIP support] mission areas. 	1. Project Initiation & Management	BCM, CIP	R
7.	The TCIPP, Version 2.0 responds to EO 13231, which tasks each federal department and agency to: <ul style="list-style-type: none"> • Integrate cost-effective security into government information systems that support national security and other essential government programs 	3. Business Impact Analysis 4. Business Continuity Strategies	BCM, CIP	R
8.	Each Departmental Office and Bureau will develop its own CIP Management Plan following the guidance	1. Project Initiation & Management	BCM,CIP	R

Ref #	Treasury Critical Infrastructure Protection Plan, Version 2, August 30, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
	<p>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.</p>			
9.	<p>Departmental Office and Bureau heads shall:</p> <ul style="list-style-type: none"> • Ensure the development of Departmental Office and Bureau CIP Management Plans that address all required information specified in the Treasury CIP Implementation Plan. • Retain overall responsibility for the assurance of critical infrastructure subject to their respective authority or control. 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. • Provide a senior representative(s) to the TIPP (Treasury Infrastructure Protection Panel). • 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. 	1. Project Initiation & Management	BCM, CIP	R
10.	<p>Departmental Office and Bureau heads shall:</p> <ul style="list-style-type: none"> • 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. • Carry out industrial security program requirements specified in TD P 71-10. • Provide data requested by the Treasury security organization on the status of their respective critical infrastructure. 	1. Project Initiation & Management	BCM, CIP	R
11.	<p>Departmental Office and Bureau heads shall:</p> <ul style="list-style-type: none"> • Establish and maintain a CIP awareness and training program. 	1. Project Initiation & Management	BCM, CIP	R

Ref #	Treasury Critical Infrastructure Protection Plan, Version 2, August 30, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
12.	Offices and Bureaus shall: 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.	8. Maintain & Exercise BC Plans	COOP, CIP	R
13.	Offices and Bureaus shall: <ul style="list-style-type: none"> • Conduct business impact assessments for critical cyber and physical assets. 	3. Business Impact Analysis	COOP, CIP, BCM	R
14.	Offices and Bureaus shall: <ul style="list-style-type: none"> • Participate in Treasury-directed continuity of operations exercises. • Report incidents/threats to the Department CSIRC. • Implement and maintain incident or intrusion monitoring and detection capabilities for their respective critical infrastructure. 	8. Maintain & Exercise BC Plans	BCM	R
15.	Offices and Bureaus shall: <ul style="list-style-type: none"> • Implement and maintain mitigation measures for their respective critical infrastructure. 	2. Risk Evaluation & Control	BCM	A
16.	Offices and Bureaus shall: <ul style="list-style-type: none"> • Ensure Treasury has current and accurate business continuity information about how CIP assets are being protected. 	8. Maintain & Exercise BC Plans	BCM	R

Statement Class

A – Advice

C - Comment

R - Requirement

B.2.2 Treasury Critical Infrastructure Protection: Interdependency Analysis Method

Ref #	Treasury Critical Infrastructure Protection: Interdependency Analysis Methodology, Version 1.1, September 24, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
1.	Business continuity is the ability to maintain constant availability of processes and information across the Treasury. [Business Continuity Planning]BCP activities involve developing a process for creating workable solutions that provide cost-effective recoverability of business functions while recognizing the high cost of providing redundancy on a continuing basis.			C
2.	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 <i>BCP</i> 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	3. Business Impact Analysis 4. Business Continuity Strategies	BCM, BRP, COG, CIP, COOP, DRP, IMP, OEP	A
3.	Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations (COOP), July 26, 1999, provides guidance to Federal Executive Branch departments and agencies for use in developing viable and executable contingency plans for the continuity of operations. The provisions of FPC 65 are applicable to all Federal Executive Branch departments, agencies, and independent organizations.			C
4.	Treasury and its Bureaus must also be in compliance with Treasury directives as well as, more current BCP guidance such as the following: <ul style="list-style-type: none"> • The Department of the Treasury Security Manual, TDP 71-10, Chapter 5, "Emergency Management Program," establishes the framework for COOP planning within the Treasury and contains specific guidance and direction to the Treasury Bureaus. • The Federal Response Plan (FRP) establishes a process and structure for a systematic, coordinated, and effective federal response to the consequences of any disaster or emergency situation in which there is a need for federal assistance. The Treasury has obligations under this plan to provide disaster relief services. 			C

Ref #	Treasury Critical Infrastructure Protection: Interdependency Analysis Methodology, Version 1.1, September 24, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
5.	<p>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:</p> <ul style="list-style-type: none"> • Prioritize business processes across the Treasury • Ensure synchronization of information technology (IT) systems and business processes. • Match recovery capabilities to known business requirements. • Provide a coordinated response to potential disaster events. • Improve security functionality and survivability of assets. • Promote more efficient use of total resources. • Fulfill legislative mandates for protecting mission-essential assets and ensuring continuity of operations. • Methodically move the Treasury’s security posture to an ideal state of mission assurance 	<p>1. Project Initiation & Management</p> <p>8. Maintain & Exercise BC Plans</p>	<p>BCM</p>	<p>A</p>
6.	<p>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:</p> <ul style="list-style-type: none"> • 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 mechanisms and how to use them. • 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 are current. 	<p>6. Develop & Implement BC Plans</p>	<p>IMP, Security</p>	<p>A</p>

Ref #	Treasury Critical Infrastructure Protection: Interdependency Analysis Methodology, Version 1.1, September 24, 2002	Applicable BC Process	Applicable BC Plans	Statement Class
7.	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, retrieveability, 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.	1. Project Initiation & Management	BCM	A

Statement Class

A – Advice

C – Comment

R - Requirement