TECHNOLOGY RECOVERY PLAN   **5325.1**
(Revised 6/14)

Introduction: The Technology Recovery Plan (TRP) is a sub-set of the state entity's Business Continuity Plan. The TRP is activated immediately after a disaster strikes and focuses on getting critical systems back online.

Policy: Each state entity shall develop a TRP in support of the state entity's Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster. Each state entity must keep its TRP up-to-date and provide annual documentation for those updates to the CISO. The annual requirements are:

1. Each state entity must file a copy of its TRP and the Technology Recovery Program Compliance Certification (SIMM 5325-B) with the CISO, in accordance with the Technology Recovery Plan Submission Schedule.

2. If the state entity employs the services of a data center it must work with the data center to establish and document TRP coordination procedures.

   Each state entity TRP must cover, at a minimum, the program areas which are listed and described in the Technology Recovery Plan Documentation for Agencies Preparation Instructions (SIMM 5325-A). If the TRP does not follow the format in SIMM 5325-A, a cross reference sheet, SIMM 5325-B, must be included with the update to indicate where required information is located.

The TRP must outline a planned approach to managing risks to the state entity's mission, including risk and potential impact to critical information technology assets. The TRP must be derived from the state entity's business impact assessment and Business Continuity Plan. Instructions for preparing the TRP are described in SIMM 5325-A.

Implementation Controls: NIST SP 800-34; NIST SP 800-53: Contingency Planning (CP)