Policy: CP0002.02	Category: Contingency Planning	Version Date: 02/22/2010
Title: **Risk Assessment - Mission Crucial Systems**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 07/08/2009
Reviewer: HSC Chief, Information Security		Next Review: 07/08/2012

Purpose:

To assess the relative criticality of specific applications, systems and data in support of other contingency plan components.

Scope:

This shall be a limited risk assessment, specifically for the purpose of determining which assets are absolutely necessary to the function of the Unit, or the loss or unavailability of which presents an unacceptable risk to the Unit's data or critical business processes. Information assets, and any other types of assets (*e.g.*, emergency power sources or cooling systems) that are absolutely necessary to the function of the Unit, or the loss or unavailability of which presents an unacceptable risk to the Unit's business processes, data or data security shall be designated as "crucial".

References:

1. Policy CP0002: Contingency Plan.
2. Standard CP0002.04: Contingency Planning Template.
3. Standard GP0003.02: Information Classification.
4. Standard GP0003.08: Report Distribution and Submission Deadlines

Policy:

1. The Unit Information Security Administrator (ISA) is responsible for ensuring an Information Technology (IT) risk assessment is conducted biannually (every two years) to identify each Unit's information assets, determine their values, replacement costs, acceptable data losses, and acceptable downtimes.
    a. Procedures in the Unit's contingency plan shall be based on this risk assessment.
        i. Any asset designated as crucial shall be specifically included in the contingency plan. Written procedures associated with the contingency plan shall address disaster preparation, recovery of functionality/availability in the immediate aftermath of a disaster, and long-term recovery and restoration to normal operation for each crucial asset. Plans for recovery of crucial assets should be very

specific and detailed, and should not assume that the local expert on the particular asset is available. The time frames for availability determined in the risk assessment shall be addressed in the plan. Use of alternative locations, alternative equipment, hot sites, etc. shall be addressed as required.

ii. For information assets not designated as crucial, the plan shall address how availability shall be restored in general terms.

b. The risk assessment shall consider the classification of the information involved and the requirements for accessing and protecting the information.

c. The contingency plan and associated procedures shall be updated during the period between biannual reviews to account for any changes in the Unit's mission, information assets, location, or any other factor which may affect the contingency plan, crucial assets, or implementation of the intent of this policy.

d. The biannual risk assessment shall be reviewed by the senior person in the Unit and maintained with the contingency plan. In alternate years between risk assessments, a review of the risk assessment shall be conducted to ensure that it is being properly updated, and that associated changes to the contingency plan are being made. A report of completion of these requirements shall be submitted annually per Standard GP0003.08, to Distribution List 2.

2. A record (which may be kept on paper or any other medium) shall be maintained for all assets designated as crucial. It shall document system outages, downtimes, failures, data loss, and major maintenance. This record shall be available for inspection by the Unit Information Security Manager (ISM), Unit ISA, and other supervisors in the Organizational Structure at any time. Data required in the record shall be per Standard CP0002.04.