

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	Business Impact Analysis Policy
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

To establish the requirements for evaluating the workflow and determining the criticality of those operations and their associated information systems within the Department of Health and Human Services (DHHS). The business impact analysis is to be an essential systematic process that is used to gather and analyze information on their functional and operational business units and processes.

Policy

The DHHS Privacy and Security Office (PSO) working with the DHHS Divisions/Offices shall perform a Business Impact Analysis (BIA) on all information systems to determine the criticality of these operations to the agency and to determine what the impacts are to the organization if those operational functions and processes were interrupted.

Roles and Responsibilities

The DHHS PSO is responsible for developing enterprise-wide procedures and guidelines on how to implement the BIA process.

The DHHS Division/Office Directors, Managers and Business Owners are responsible for determining the criticality of their operations. Each DHHS Division/Office is responsible for ensuring that contingency plans have been implemented. The BIA is used to accomplish this objective and is used to analyze the service workflow, which typically consists of both manual and automated (Information Technology Services (ITS)) components.

Implementation

The DHHS PSO shall:

1. Provide implementation guidelines and support. Policy implementation shall be based upon the use of management-approved security standards and follow requirements established by IT Services.

2. Develop the BIA process to be followed by the divisions/offices and assist in determining criticality and impact assessment.
3. Define a method of evaluating data. The BIA shall accomplish the following activities:
 - A. Identification of critical functions and services.
 - B. Identification of resources (technology, staff and facilities) that support each critical function or service.
 - C. Identification of key relationships and interdependencies among the impacted functions and services.
 - D. Estimated decline in effectiveness over time that a critical function or service can be inoperable without a catastrophic impact.
 - E. Estimated maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
 - F. Identification of any interim or workaround procedures that exists that are needed to perform critical functions or services.
 - G. Identification of any critical events or services that are time-sensitive or predictable and require a higher than normal priority.
 - H. Identification of any critical non-electronic media required to support critical functions or services.
4. Provide BIA oversight for the divisions/offices

The DHHS Division/Offices shall adhere to the following requirements:

1. Identify Stakeholders – The manager(s) and system owner(s) shall participate as well as key individuals who are knowledgeable of both the business operations and ITS operations.
2. Establish Criticality Levels – DHHS Divisions/Offices shall establish three (3) levels of criticality for its information systems. They are:
 - A. High – Critical systems are those that support essential services. These systems must be available with minimum downtime (i.e., 48 hours or less) since the lack of availability will have a significant impact on those receiving services from the agency.
 - B. Medium – Important systems are next in priority since a temporary loss (i.e., two (2) to seven (7) days) of service will have minimal impact on those receiving services.
 - C. Low – Systems that are not providing a time-critical service. These services can be suspended for a reasonable period of time (i.e., one (1) or two (2) weeks) resulting in minimal disruption to the organization.
3. Adopt BIA Process/Standards/Tools – The DHHS Divisions/Offices shall adopt the BIA process developed by the DHHS PSO.

Standard tools and methodologies as required by ITS shall be integrated into this process by the DHHS PSO.

4. Planning – A formal plan for determining the criticality of operations and performing an impact assessment shall be developed under the guidance provided by the DHHS PSO. This plan shall be approved by management and include milestones, schedules and resources needed.
5. Data Collection – The DHHS Divisions/Offices will follow the DHHS PSO plan for collecting data. Methods available to collect data or to set up the data collection plan, for BIA purposes include:
 - A. Questionnaires
 - B. Facilitated Data Gathering Sessions
 - C. Process Flows and Interdependency Studies
 - D. Risk Assessments
 - E. IT Application or System Logs
 - F. Financial Data
 - G. BCP Audit Documentation
 - H. Production Schedules
6. Performing Impact Assessments - The BIA provides DHHS Divisions/Offices with reliable data concerning potential impacts and costs, establishes the basis for setting priorities, and helps select the proper strategy for recovery. The BIA shall consider the following impacts:
 - A. Financial Impact of the Business Impact Analysis. The financial impact assessment of each business process, function, or workflow shall consider the revenue loss estimate based upon the lack of availability. There shall also be an estimate of the extraordinary expense impact – including the acquisition of outside services, emergency purchases, rental/leased equipment, or relocation expenses for employees.
 - B. Operational Impact from the Business Impact Analysis. The operational impact assessment of each business process, function, or workflow shall be considered in determining the estimated business interruption costs.
 - C. Technological Dependence. The technological dependence assessment for each business process, function, or workflow shall consider the interdependencies of the process/function/workflow on other systems.
7. Documentation - A BIA Report shall be developed with the assistance of the DHHS PSO. This document should have an executive summary, the determination of criticality, impact assessment and supporting data.

8. Communications - The BIA Report shall be sent to the appropriate parties to ensure that the information is used in Business Continuity/Disaster Recovery Planning.
9. Maintenance – The DHHS PSO shall ensure that BIA planning is an integral part of the divisions/offices ongoing disaster readiness planning process.

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer (DHHS.Security@ncmail.net). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)

Exceptions

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [ITS Waiver and Appeals Policy](#).