U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY
DOT H 1350.254

DEPARTMENTAL GUIDE TO CONTINUITY OF OPERATIONS PLANNING

TABLE OF CONTENTS

DEPARTMENTAL GUIDE TO CONTINUITY OF OPERATIONS PLANNING

PURPOSE

The purpose of this Guide is to provide Department of Transportation (DOT) and their Operating Administration managers, ISSO's and network administrators with a step-by-step approach for preparing a Contingency Plan, which address short term losses, or a

Continuity Plan, which addresses long term losses, for their systems. These completed plans will allow the organization to address the steps to be taken in order to maintain the operation of their critical functions, in the event of contingencies, losses, disruptions or disasters.

SCOPE

The provisions of this Guide apply to the Department of Transportation (DOT), its Secretarial Offices and Operating Administrations.

GOALS

The Goal of continuity of operations planning is to provide reasonable methods to conduct prevention, response, resumption, recovery or restoration services, should events occur which prevent normal operations. The contingency and continuity plans must be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption or denial of service. At a minimum, these plans should be tested on an annual basis.

REFERENCES

The DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.2 implements statutory and regulatory Information Resources Management (IRM) and security requirements for the Department. It also calls for ensuring the confidentiality, integrity, and availability of information contained, processed, or transmitted in/on sensitive systems. Refer to DOT H 1350.2.1 REGULATORY AND GUIDANCE DOCUMENTS for specific references.

OVERVIEW OF CONTINUITY OF OPERATIONS PLANNING

Like other government agencies, DOT depends on the availability of accurate and timely information to manage a broad range of programs and budgets with far-reaching effects. Virtually all-vital information is processed in some form by computers. Hence a key aspect in DOT's overall risk management program must be the ability to respond to unplanned, adverse situations that may destroy, damage, degrade, or compromise information systems data or computer processing capabilities so that essential operations may continue. Ensuring that this ability exists, and is indeed viable (proven via periodic testing) is the major function of continuity of operations planning.

OMB Circular A-130 requires continuity of operations planning for every information system. This includes both contingency planning (short-term), and continuity planning (longer-term), in order to rapidly and effectively deal with the potential disruption of critical mission and business functions. To avert these disruptions, or minimize their damage, organizations must take proactive steps to develop a Continuity of Operations Plan (COOP). The Contingency portion of the COOP focuses on minimal, day-to-day outages (server down, localized short-term connectivity loss, etc.), while the Continuity portion deals with long term or disaster scenarios. The COOP contains operational recovery issues, ranging from arrangements for a limited backup capability (needed files, programs, paper stocks, pre-printed forms, etc.) to relocation to a different facility in the event of a total failure. The goal is to protect lives, limit damage to property, and minimize the impact on operations, including information systems processing activities.

CONTINUITY OF OPERATIONS PLANNING PROCESS

Continuity of operations planning involves more than planning for a move offsite if a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in case of disruptions, either long or short term in duration. The continuity planning process is covered in six steps:

Step 1 - Identify Mission- or Business-Critical Functions.

Step 2 - Identify Resources that support Critical Functions.

Step 3 - Anticipate Potential Contingencies or Disasters.

Step 4 - Select Continuity Of Operations Planning Strategies.

Step 5 - Document Continuity Of Operations Strategies.

Step 6 - Test and Revise Strategies.

Each of these steps is described in detail in the following paragraphs.

A. Step 1. Identify Mission- or Business-Critical Functions.

The definition of an organization's critical mission or business function is called a business plan. Because the development of the business plan will be used to support the continuity of operations planning process, it is necessary, not only to identify critical missions and business processes, but also to set priorities and time criticalities for them. The system owner is responsible for ensuring the completion of the business plan and for prioritizing the resumption, recovery or restoration needs for the organization's critical functions. Because a fully redundant capability for each function is prohibitively expensive for most organizations, certain functions will not be performed in case of a disaster. If appropriate priorities have not been set, it could make a difference in the organization's ability to survive a disaster.

1. Mission Statement. Government departments, divisions, and offices generally have a formal statement concerning the mission to be performed. These statements may be contained in departmental policies or directives, handbooks, or public information guides. Regardless of the source, the criticality determination process starts with an overall mission statement which identifies what the office is responsible for doing. For example, as its primary mission, an office or IT System within the United States Coast Guard (USCG) may be responsible for licensing the vessels for commercial and charter fishing (see Figure 1).

2. Office Functions. The mission statement is usually a generalized description of why an office exists. It does not describe what function an office performs to accomplish the mission. Using this same example, the commercial/charter fishing boat office may be required to process applications for licenses, investigate and inspect the firms, develop and issue regulatory guidelines, etc. Special requirements affecting the performance of the function or relating to the information involved (e.g., Privacy Act protection) should also be noted.

Figure 1, Mission Statement Example

3. Functional Activities Listing. The process continues by developing a list of all functions performed by the office in support of the mission. In parallel with this listing, it is also necessary to identify those functions that require support from IT Systems, and the extent of that dependency (i.e., is the function totally dependent on IT System support, is only some portion that can be

quantified dependent on such support, or could the function be performed manually with little or no loss of efficiency). Any special requirements affecting the performance of the function or relating to the information involved should also be noted. These could include the sensitivity of data, or whether there is a specific timeframe when data is more critical than other times.

Appendix A, Tab A contains an Office Mission/Functionality Matrix Template that is designed to aid in this definition process. A sample matrix, which has been filled in based on the USCG example given above, is contained in Figure 2.

4. Criticality Matrix. The next element is the development of a criticality matrix. Criticality guidelines must be developed which identify those office functions that deal with aspects that are critical to any government agency, and the time frames that must be associated with those factors. Developing a matrix, similar to that used for determining sensitivity and protection requirements in system security plans, is one approach to determining IT System criticality. Most DOT offices and operating administrations are not involved with the more obviously critical factors, such as saving lives or national defense. They will have to develop an office-specific list of critical functions. The primary objective is to identify only those essential functions that, if not performed, will cause the greatest loss to the office in terms of the inability to operate, the expenditure of additional funds (other than those directly associated with restoring the office after a disaster), or embarrassment to the Federal Government, DOT or the operating administration.

In the event that there are no specifically identifiable critical factors, the COOP planner and senior office officials must develop a list of criticality guidelines that will assist in prioritizing all office functions. These guidelines should permit each function to be evaluated in terms of the importance of the function in accomplishing the mission of the office, and how quickly this function must be performed. The longer the function can do without IT support, the less critical is the supporting information system, --- hence criticality is a function of time.

Figure 2, Sample Office Mission/Functionality Matrix

Tab C in Appendix A contains a sample Office Function Criticality Matrix. To help illustrate the process, Figure 3 shows the Matrix filled out for the USCG example.

5. Criticality Determination. The next part of the process is to compare the functional activities against the criticality determinations and corresponding time frames. In a COOP, functions that do not require IT support (e.g., the deliberations of an adjudication board) are still critical. A COOP is concerned with all essential functions and may go beyond those functions requiring only IT processing. All office functions are compared against the criticality determinations and time factors, and against each other. The result is a prioritized list of essential activities, based on criticality, and reflected in terms of the maximum time frame that these essential functions are not performed before the office fails to accomplish its mission.

In the COOP, functions that do not require ITsupport may be separately identified by the COOP planner. The prioritized list of IT system-supported functional activities is then based on the time frame the supporting system can be unavailable due to lost, damaged or destroyed data and/or hardware.

Figure 3, Office Function Criticality Matrix Example

This distinction has been added to account for situations in which less-than-catastrophic damage to the primary site has occurred. The matrix can be further modified to identify specific systems, applications, and/or databases if a function is supported by more than one, or if a given system, application, or database is more critical to the effective completion of a given function.

B. Step 2. Identify Resources That Support Critical Functions.

After critical missions and business functions are identified, supporting resources should be identified, as well as the timeframes in which each resource is used, and the effect of unavailable resources on the missions. It is important to note that the COOP resources inventory must consist of only those physical resources and support services necessary for an office to perform the essential parts of its mission. The COOP does not plan for the immediate or even eventual replacement of all existing resources at an alternate site. Rather, it is intended to implement a viable and effective office in an alternate location for an undetermined period of time to perform only those functions essential to the mission.

In addition to precisely identifying the minimum levels of resources required to activate a temporary office, the resources inventory must also identify who is responsible for each category of items, where the existing items are located (and if backup supplies already exist, where they are located and in what quantity), what and where is the source of replacement or re-supply, and in some instances, what is the cost and time frame for replacement. The resources inventory is not a static document, even during development. As COOP planning progresses, preparatory actions will instigate the modification or expansion of certain inventory data.

Continuity of operations planning should address all the resources needed to perform a function, including:

1. Human Resources. Human resources include both operational/support personnel and system users. Some functions require personnel with special expertise or training, while others require lesser skill levels.

2. Processing Capability. Traditionally, contingency planning has focused on processing power. Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks.

3. Automated Applications and Data. DOT information systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors.

4. Computer-Based Services. DOT uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice; however, in many organizations these are managed by the same service. Information services include any source of information outside of the organization. Many of these sources have now become automated, including on-line government and private databases, the Internet and external EMail.

5. Physical Infrastructure. Physical infrastructure elements include a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need

space and utilities, such as electricity. Electronic and paper media used to store applications and data may also have specific physical requirements.

6. Documents and Papers. The performance of many DOT functions relies on vital records and various documents, papers, or forms. These records could be important because of a legal need, or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

Appendix B contains a Critical Resources Inventory Outline that may be used to assist in the identification of critical resources. Also see the following tables for a methodology of matrixing this information. As showing in the table the "QTY 1, QTY 2, QTY 3, etc" fields can be used to identify the quantity of personnel, services, supplies, equipment, etc. needed as the criticality timeline continues. This will also aid in budgeting for a period of coverage to ensure that a percentage of the resources are available.

Supplies Worksheet											
Item	**Description**	**Color**	**Model / Serial Number**	**Unit Cost**	**Qty 1**	**Qty 2**	**Qty 3**	**Qty 4**	**Qty 5**	**Total Needed**	**Total Cost**
										0	$ -

Software Requirements Worksheet									
Make	**Version**	**Unit Cost**	**Qty 1**	**Qty 2**	**Qty 3**	**Qty 4**	**Qty 5**	**Total Needed**	**Total Cost**
								0	$ -

Hardware Requirements Worksheet									
Make	**Model**	**Unit Cost**	**Qty 1**	**Qty 2**	**Qty 3**	**Qty 4**	**Qty 5**	**Total Needed**	**Total Cost**
								0	$ -

C. Step 3. Anticipate Potential Contingencies or Disasters.

Although it is impossible to anticipate everything that can go wrong, this step involves identifying a likely range of problems. Developing scenarios can help an organization to prepare a plan that addresses a wide range of possible mishaps. Scenarios should include small and large disruptions that require both short-term (contingency) and long-term (continuity) solutions.

D. Step 4. Select Continuity Of Operations Planning Strategies.

This step considers the use of contingency and continuity plans to recover needed resources. When alternative strategies are evaluated, current controls for preventing and minimizing losses should be considered. Because no one set of controls can prevent all losses in a cost-effective manner, prevention and recovery efforts should be coordinated. Risk assessment can also help determine an optimal strategy. A contingency planning strategy normally consists of five parts:

prevention, response, resumption, recovery, or restoration of services. Prevention refers to those measures taken to forestall a disruption of service (e.g., preventive maintenance, virus prevention, etc.). Emergency response encompasses the initial actions taken to protect lives and limit damage. Resumption refers to the steps taken to continue support for critical functions. Recovery concerns the re-activation of a greater scope of business processes and services beyond the most time-sensitive processes. Restoration is the return to normal operations. The longer it takes to restore normal operations, the longer the organization will have to operate in the resumption or recovery mode. The selection of a strategy needs to be based on practical considerations, including feasibility and cost. Different categories of resources should be considered:

1. Human Resources. During a major continuity plan implementation, people will be under significant stress and may panic. If the continuity plan is implemented as the result of a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used. However, the use of additional personnel may introduce security vulnerabilities. Whereas in the implementation of the contingency plan can in some cases be seamless and there could be no difficulty of a Human Resource nature.

> Remember, continuity of operations planning, especially for an emergency response, normally places the highest emphasis on the protection of human life.

2. Processing Capability. For less serious contingencies, processing capabilities can be restored from backups or original media, by repairing equipment components, or by purchasing new equipment. Federal agencies have the authority to issue Purchase Orders to quickly acquire needed equipment and supplies in limited quantities. This authority is usually limited between $25,000 and $50,000, but is sufficient to acquire "off-the-shelf" hardware and software. Essential hardware could be acquired by Purchase Orders in one of two ways: purchase of replacement or upgraded equipment and lease of essential equipment for a limited period of time. The outright purchase of identical replacement hardware is the most obvious use of the Purchase Order option. However, the purchase of upgraded equipment is a reasonable alternative, given the fact that the existing equipment may not be economically salvageable. On the other hand, the short-term lease of essential equipment to augment or temporarily replace existing equipment during salvage operations provides a cost-effective alternative. There is however a risk involved with the leasing of equipment that must be addressed in both the contingency and continuity plans. That risk is the fact that those systems must be thoroughly scrubbed to ensure the protection of information that has been stored or processed on these machines. Although these two options could offset the lack of facilities and equipment at the time of a disaster, they are subject to the disadvantages of high cost and long preparation time. In a widespread disaster, the requirements for space, hardware, communications, etc., could temporarily exceed the demand. These two options must also be used in combination because neither provides for both facilities (to include associated utilities and communications) and equipment, furnishings, and supplies.

Also for less serious contingencies, planners should consider the use of an overall in-house backup strategy. In-house backup is the use of under-utilized facilities and/or additional equipment (i.e., older equipment still on-hand and/or new equipment awaiting installation) controlled by the affected activity or by its superior or subordinate activities. In-house backup maximizes the use of suitable space and equipment, or space and equipment that is capable of being upgraded in a very short period of time to support continuity of operations activities. DOT activities are required to identify and make available under-utilized IT equipment to other agencies under normal conditions. Although not usually done with PCs/LANs, the principle is similar. This same equipment could be earmarked for use in a continuity of operations situation. Pre-determined backup equipment alternatives (e.g., leasing) would have to be included in the plan to allow for the fact that the in-house equipment may not be available at the time of the disaster.

For a serious contingency or continuity event, however, the strategies for ensuring processing capability are normally grouped into five categories:

(a) Hot Site. A hot site is a building already equipped with processing capability and other services. Operational standby facilities require a subscription contract and charge various fees. Normally, a three or five-year contract is negotiated and includes a specific hardware and software configuration with detailed communications requirements, which must be updated whenever changes occur. Subscription fees are determined by these requirements. The reduction in costs for the minimum essential capabilities required by a COOP is not significant and may not be warranted for continuity of operations. Another potential drawback for the IT user is that these services are relatively new and not widely dispersed. Therefore, a Hot Site facility may not be conveniently located.

(b) Cold Site. A Cold Site is a building for housing processors that can be easily adapted for use. Such a facility may be owned by DOT or a DOT operating administration, owned by another government agency (e.g., DOD, GSA, etc.), or Government-leased for one or more departments or operating administrations. In the event of a disaster situation, the affected office(s), in conjunction with hardware vendors, acquires and installs the essential AIS hardware, software, and communications. Cold Sites are more practical for AIS-type operations since a shell facility may be owned by DOT or the facility can be virtually any office space with sufficient electrical power, communications line capability (installed or capable of being installed during a disaster situation), and regular air conditioning. AIS hardware is more readily available, more easily shipped, and more easily installed.

A Cold Site may also be supported by a special equipment contract (if not already in-place as part of a standard hardware maintenance agreement). There are a number of hardware vendors who offer guaranteed delivery and set-up within 24 hours. Although the maintenance costs are somewhat less than an operational standby, they represent a continuing expense. For IT activities, consideration should be given to leasing essential computer equipment and peripherals to augment equipment salvaged from the primary site or to temporarily replace essential hardware until the primary site can be restored without additional disruption to IT configuration. Leasing eliminates the on-going maintenance costs of a special equipment contract, but does not provide for the guarantees that appropriate equipment will be available when needed or within required time frames. As described earlier leasing also creates the problem of data security, as special precautions must be taken to ensure that all data that has been stored or processed on the system has been removed from the leased equipment. This practice requires more than a simple deletion of the data as deleted files can be detected, identified and restored. The site availability time frame, which includes hardware, communications, and equipment installation, may not meet organizational or system requirements as set forth in the contingency or continuity plans.

(c) Redundant Site. A redundant site is a site equipped and configured exactly like the primary site

(d) Reciprocal Agreement. A reciprocal agreement is a formal agreement that allows two organizations to back up each other. The agreement is usually with an external agency, for the two to provide backup AIS processing support to one another in the event of a disruption in primary processing support. The external office, division, operating administration, or department is not in the business of providing IT processing support, but agrees to provide reciprocal support in recognition of mutual backup requirements.

Although low development and maintenance costs are the principal advantage to this alternative; consideration must be given to establishing an agreement with an organization that will not be affected by the same disaster. Reaching an agreement with another activity, such as a counterpart office in another division or operating administration, provides no effective continuity

of operations capability if that activity is affected by the same disaster. The activities establishing a mutual assistance agreement should be geographically separated.

This does not preclude reaching an agreement with another DOT activity. Satisfactory agreements can be reached between superior and subordinate levels (e.g., DOT and one of its operating administrations) or between equivalent levels (e.g., two operating administrations), so long as the geographical separation of sites is achieved. This in-house arrangement would mitigate operational/legal problems resulting from the failure of one party to execute the agreement because the aggrieved party could appeal to a common superior.

The biggest disadvantage of the mutual assistance agreement is that, "*Their disaster becomes your disaster.*" Many of the disadvantages noted above identify areas of hardship and general inconvenience to both activities. Without a specific system, site, and pair of organizations in mind, it is difficult to evaluate a mutual assistance agreement alternative completely and fairly.

Remember that mutual assistance agreements are not considered viable solutions without a formal agreement outlining all conditions and signed by individuals in positions of authority to uphold the agreement.

(e) Hybrids. Any combinations of the above, such as having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

In addition to these five alternatives, another approach readily available to IT environments is to allow employees to work at home (telecommute). Personally owned PCs and modem connectivity have become commonplace. Even limited use of this alternative would ease the continuity of operations burden by reducing or eliminating the need to provide suitable office space and to acquire hardware and/or software assets. In addition to reduced costs, it offers the advantage of immediate availability. Also, it can be thoroughly tested. However, there are disadvantages, too. Not all employees can be expected to have suitable hardware and/or software or modem connectivity. Technical and maintenance support to privately owned property poses legal difficulties and limits sustainability, while information security and anti-viral protection are significant problem areas.

Figure 4 presents a set of evaluation characteristics that may be used to help weigh the alternatives for handling Processing Capability.

Evaluation Characteristic	Planning Considerations
Compatibility	Hardware, software, and communications that are or would have to be installed at the alternate site must be the same as or compatible with original equipment supported.
Accessibility	The alternate site must be readily accessible, but not so close as to share the same disaster.
Reliability	The alternate site must be capable of supporting the operations of the affected office(s) 24 hours a day, seven days a week. Maintenance for site equipment, hardware and communications should be on-site or on-call.
Capacity	The alternate site and facility/computer equipment must have sufficient floor space, heating/cooling/power, communications lines, and memory capacity to support the suite of equipment required.
Security	The physical security at the alternate site must be sufficient to protect the sensitivity of the information and data.
Time to prepare	There must be sufficient time to prepare for the disaster, including time to prepare/convert data and software, prepare the site, prepare/store supplies, forms and documentation, obtain/install power and communications circuits, and prepare and test the COOP.

Support & assistance	There must be on-site technical support and assistance to set-up and configure the hardware, software, and communications.
Cost	Cost factors can be subdivided into three categories: • Preparation costs include cost of any equipment or LAN/WAN. • Maintenance costs include hardware, software, or telecommunications maintenance/lease fees. • Execution costs are incurred in declaring a disaster and executing the COOP, including rent, travel, and per diem.

Figure 4, Processing Capability Evaluation

3. Automated Applications and Data. Normally, the primary contingency and continuity strategy for applications and data is regular backup and secure offsite storage. Important issues to be addressed include the frequency of backups, the frequency of offsite storage, and the manner of transporting backups. Office policy should require the AIS or LAN administrator to maintain separate master copies of all operating system and specific application program software, update these masters immediately upon implementation of approved changes, and store these masters in a secure off-site location, together with copies of all applicable hardcopy documentation and operating manuals. A similar policy should require the appropriate individual(s) to prepare backup copies of all electronic files on a regular (e.g., not less than weekly) basis, to maintain copies of all required references and hardcopy files, and to store the backup copies in a secure off-site location. In an AIS environment, the volume of equipment/supplies to be stored is relatively small based on the nature of the media involved (diskettes and 8 mm cartridge tapes). The DOT Data Center makes provisions to store these types of materials in support of DOT activities. This provides a ready solution for magnetic media. Hardcopy data could be stored on a permanent retention basis in local operating administration, DOT, or general Federal storage facilities.

4. Computer-Based Services. Communications is also a key discriminator in selecting an appropriate COOP alternative. Incompatible communications and/or insufficient lines will disqualify a site or option. The COOP planner must ensure that adequate compatible communications are available at the alternate site, or that they can be provided during a disaster situation. If not already present, an agreement with the communications vendor must be negotiated. This agreement must cover all necessary voice, data, and image communications. Separate agreements must also be negotiated with equipment vendors for modems, facsimile machines, telephones, encryption devices and keys, if required.

Service providers may offer contingency services. Voice communications carriers often can reroute calls to a new location, and data communications carriers can also reroute traffic. Local voice service may be carried via cellular phones. If one service is down, it may be possible to use another. Resuming normal operations may require rerouting of communications.

5. Physical Infrastructure. Arrangements must be made for processing capability support, office space, furniture, and more. If the COOP calls for moving offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new permanent location. A related alternative available to Federal agencies is the U.S. Government's procurement system. The General Services Administration (GSA) has the responsibility of acquiring additional office space on an "as required" basis for Federal agencies, and the responsibility of managing standing contracts for goods and services. Because minimal space is

required for continuity of operations activities, this capability permits fairly rapid acquisition of space without the "overhead" costs of rents or subscription fees.

6. Documents and Papers. The primary contingency strategy is usually backup onto magnetic, optical, microfiche, or other medium and offsite storage. A supply of forms and other needed papers can be stored offsite. Backup storage space should be located close enough to the primary site for convenience in placing items into storage on a regular basis, but not so close that it will be affected by the same disaster. On-site (i.e., same office/building) storage is not acceptable.

E. Step 5. Document Continuity Of Operations Planning Strategies.

With continuity of operations strategies well defined, the next step is to create the COOP itself. The COOP needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a continuity of operations event, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the COOP in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities. A model COOP is contained within Appendix C of this Guide. The structure of the COOP includes:

- Plan Overview – consisting of an introduction, statement of policy, objectives, scope, assumptions, recovery strategy and plan administration responsibilities.

- Continuity Process Overview – outlines the four major stages of the process (emergency response, resumption, recovery and restoration), including the central activities and objectives of each stage, and the relationships among stages.

- Continuity Team Organization – defines the specific organization set up to work towards survival and the resumption of time-sensitive business operations. The teams associated with this plan represent office functional units and/or or support functions developed to respond, resume, recover or restore operations of the facility. Each team is comprised of individuals with specific responsibilities or tasks that must be completed to fully execute the plan. Figure 5 presents a representative example of a Continuity Team Organization Structure.

Figure 5, Representative Continuity Team Organization Structure

- Plan Maintenance – including both scheduled and unscheduled maintenance, as well as a periodic re-evaluation process. Scheduled maintenance consists of quarterly reviews and updates as well as annual structured walk-through and/or tactical exercises (as described in the Plan Exercise section below). The purpose of the plan review is to determine whether changes are required to strategies, tasks, procedures, the continuity organization, and notification procedures. The majority of unscheduled maintenance activities occur as the result of major changes to service level agreements, hardware configurations, networks, production processing, etc. The Continuity Plan maintenance process should also include a periodic re-evaluation of the minimum hardware capacity required to provide short-term response, resumption, recovery and restoration capability. The re-evaluation process must address the capacity growth requirements associated

with the increase of transaction processing volumes of the production application systems, as well as the addition of new systems to the production environment.

- Plan Exercise – consisting of the various types and scope of exercises designed to test and evaluate the COOP. Exercises should be conducted when a major revision to the plan has been completed, when additional production systems are implemented, when significant changes in systems, applications and/or data communications have occurred, and when the preparedness level of continuity teams must be verified. Exercises may include structured walk-throughs, tactical exercises, live production exercises, simulations and announced/unannounced exercises.

The details for plan execution reside in Appendices to the COOP itself. These Appendices contain the specific data required by the various Teams in order to perform their designated roles during each stage of the process. Appendices include:

- Priority Contact List – including employee names and contact information.

- Employee/Contractor Notification List – containing a directed list of who is to contact who regarding the communication of continuity information (see Figure 6).

Figure 6, Sample Notification List

- Team Member Roster – identifies the specific individuals belonging to each Team, and their contact information, as shown in Figure 7.

- Team Task List with Dependencies – consists of a detailed, step-by-step listing of each task to be performed by the members of the various continuity teams. Where a specific task must await action by a member of another team, this is so noted, and the task/responsible individual is identified. This area is key to the entire COOP. Figure 8 contains an example of a portion of a Team Task List. Each task is also separately identified by a unique number that identifies both the team and the order of execution. Additionally, the task sheets contain room to check off task completion, and the expected/actual times to complete.

- Enterprise Process Configuration – lists, for each IT System or Process, the associated software, equipment, supplies, network Information and responsible Teams, as illustrated in Figure 9.

- Vendor Representatives – contains a listing of all applicable vendor contact information, including local representatives and focal points within the organization. An example is shown in Figure 10.

Figure 7, Team Member Roster Example

- Location Information – contains the location of all off-site storage, alternate operating locations (hot or cold sites) record repositories, etc. Driving instructions and personnel focal point contact information is also included for each location.

- Vital Records – includes a listing of all necessary documents, manuals, diskettes, CD-ROMs and all other media necessary to implementing the COOP.

F. Step 6. Test and Revise Strategy.

A COOP should be tested in order to train personnel, and to keep the plan in step with changes to the environment. The extent and frequency of testing will vary among organizations and systems. There are several types of testing:

1. Review. This is a simple test to check the accuracy of the COOP. For instance, a reviewer can check the accuracy of contact telephone numbers, building and room numbers, and whether the listed individuals are still in the organization.

2. Analysis. An analysis may be performed on the entire plan or parts of it. The analyst may mentally follow the strategies in the COOP and look for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to detect missing or unworkable pieces of the plan.

Figure 8, Team Task List Example

Figure 9, Enterprise Process Configuration List Example

Figure 10, Sample Vendor Representative List

3. Simulation & Test. Simulation and test consists of various types and scope of exercises designed to test and evaluate the COOP. In the Structured Walk-through, a disaster scenario is established, and the teams "walk-through"their assigned tasks. This is a role-playing activity that requires the participation of at least the team leaders and their alternates. A Tactical Exercise is a simulated exercise, conducted in a "war game" format. All members of the continuity organization are required to participate and perform their tasks and procedures under announced or surprise conditions. The exercise monitor provides information throughout the exercise to simulate events following an actual disaster. In a Live Production application system exercise, an operating system is brought to live status on the alternate processor(s), and the data communications network is switched to the alternate site. All resources, other than the computer and communications hardware needed to support this exercise, must be retrieved from the off-site storage facility. A simulation requires the execution of notification, operating procedures, the use of equipment hardware/software, possible use of alternate site(s), and operations to ensure proper performance. Simulation exercises can and may be used in conjunction with checklist exercises for identification of required plan modification and staff training.

Announced exercises are scheduled exercises generally involving actual resumption of computer processing at the alternate computer facility. Production processing is usually not interrupted, but may be planned for actual resumption and validation at the "Hot Site." This type of test usually involves the entire continuity organization, including selected users along with operations and technical staff. Unannounced exercises are surprise technical exercises that require processing to be actually recovered at the alternate site. Production processing continues in parallel and is not interrupted. This type of test generally involves only a small portion of the continuity organization and few, if any, users

To ensure that testing is performed in a cost-effective manner, while still accomplishing the objective of validating the COOP, a separate test plan, with specific scenarios and outlines of

acceptable responses, should be developed and followed by the management representatives, such as the team conducting the test.

Regardless of the type of testing performed, documentation of the test must be forwarded to the ISSO and maintained on file within the organization until Senior Management or System Owners review the documentation.

Because the plan will become dated as time passes and resources change, responsibility for keeping the COOP current should be specifically assigned. Maintenance of the plan can be incorporated into procedures for change management so that upgrades to hardware and software are reflected in the plan.

APPENDIX A: IT SYSTEM CRITICALITY QUESTIONNAIRE

A.1. GENERAL

A key aspect in the continuity of operations planning process is to identify what functions and AIS IT supporting systems are performed and to determine how critical these functions are to the overall mission. Information sensitivity and criticality are not the same. Not all functions are critical or critical one-hundred percent of the time. An effective COOP will allow for these situations by identifying all functions, establishing criticality criteria, and then prioritizing the functions and supporting AISIT systems. *Only the most critical functions and systems (i.e., mission essential functions) are considered in continuity of operations planning.*

A.2. PROCEDURES

Sample forms for accomplishing the following procedures are attached as Tabs A and B to this Appendix.

A.2.1 Mission Statement: Enter the office mission statement provided by the senior official responsible for the overall operations of the affected office. (See Tab A.) Remember, this is a general mission statement, not a listing of office functions, *i.e., why does this particular office exist?*

A.2.2 Functional Activities Listing: List all of the functional activities, as identified by the senior office official and key end-users, that the office performs to accomplish the mission. (See Tab A.) *Ensure that all functions are listed and a record of OAIS ITsupport and other special requirements is developed.*

A.2.3 Criticality Matrix: Development of the criticality matrix is a two-part process:

- First, determine why any of the office functions are critical.

  - List key criticality factors or guidelines developed by the senior office official.

  - Enter each function and supporting system, identified in the Functional Activities Listing, next to the appropriate criticality factor.

  - Determine, in terms of time (minutes, hours, days), how long the system supporting that function can be "out of service" before mission failure occurs.

- If there are a number of similar functions and systems for the same factor, consider weighting the factors. The total of factor weights will determine the priority order of factors. The priority order of functions will be determined by the time frames in which each must be re-established.

- Second, develop the final Office Function Criticality Matrix (See Tab B.). Enter individual functions in descending priority order based on their criticality time frames. In an IT environment, it is necessary to account for less-than-catastrophic situations. Therefore, the time frames of the loss, damage, or destruction of data and/or hardware must be considered separately.
- Third, determine which of the critical functions are absolutely essential to accomplishing the office mission. These functions and systems will be the only ones supported under the COOP.

MISSION STATEMENT:								
Functional Activity	**IT Support Required**		**IT Dependency Level (%)**				**Special Requirements**	
	YES	**NO**	**0-25**	**26-50**	**51-75**	**76-100**	**Sensitive (Y/N)**	**Periodic (Time)**

TAB A: OFFICE MISSION/FUNCTIONALITY MATRIX

CRITICALITY FACTORS/TIME FRAMES

FACTOR	FUNCTION	TIME FRAME					
		IMMEDIATE	SHORT TERM	MEDIUM TERM	LONG TERM	CONTINUOUS	PERIODIC
LIFE SAVING							
NATIONAL DEFENSE							
PUBLIC SAFETY							
LAW ENFORCEMENT							
FINANCIAL							
MANDATED							
EXTERNAL SUPPORT							
INTERNAL SUPPORT							
ROUTINE ACTIVITIES							
SPECIAL TASKS							
OTHER							

TAB B: CRITICALITY FACTORS/TIME FRAMES

FUNCTION CRITICALITY MATRIX				
Functional System/ Application	**Criticality**			**Adverse Situation (Data/ Hardware)**
	HIGH - Hrs*	**MEDIUM - Hrs***	**LOW > Hrs***	
				Lost
				Damaged
				Destroyed
				Lost
				Damaged
				Destroyed
				Lost
				Damaged
				Destroyed
				Lost
				Damaged
				Destroyed
				Lost
				Damaged
				Destroyed
				Lost
				Damaged

				Destroyed

TAB C: OFFICE FUNCTION CRITICALITY MATRIX

APPENDIX B: IT SYSTEM CRITICAL RESOURCES INVENTORY OUTLINE

B.1 GENERAL

The COOP must provide for the re-establishment of only those office assets necessary to support essential operations. Determining the specific resource requirements begins with a critical review of existing resources. Following the inventory, the COOP planner, office senior official, and key end-users must determine the minimum resources required to establish a viable, effective office in an alternate location for an undetermined period of time.

B.2 INVENTORY PROCEDURES

There is no specific format for developing a critical resources inventory. In terms of physical property, the existing property inventory provides most, but not all, of the information required. There are key items of information that must be included in the resources inventory.

B.2.1 Facilities: The inventory must specify the current location(s) of all office functions and the minimum floor space required. (NOTE: COOP site floor space will not equal existing floor space, but must provide for the minimum essential requirement.) If the office receives routine support from other activities within the same division or operating administration (e.g., copier support, mailroom), that will be required but will not be readily available, provisions for obtaining for this support must be taken into account.

B.2.2 Hardware: The inventory must provide a full description of all IT hardware and peripherals, a specific location, and a description of any special features or requirements. If known, the inventory should also provide replacement cost or original purchase/lease cost. Finally, the inventory must indicate the criticality factor and time frame for each item, as well as the replacement source.

B.2.3 Software/Applications: The inventory must provide a full description of all IT operating system software and applications, specific location/systems, the individual responsible for the software, use or list of functions supported, source, replacement cost, and a description of backup procedures and backup storage location. The inventory must also indicate the criticality factor and time frame for each item.

B.2.4 Databases: The inventory must provide identifying information on each database, specify the owner and/or individual responsible, describe backup procedures and locations, and describe its use(s) and application(s) supported. The inventory must also indicate the criticality factor and time frame for each item.

B.2.5 Documentation: The inventory must provide a full description of each item of required documentation (including hardcopy information), identify the individual responsible for the

documentation, describe backup procedures and identify backup location(s), and denote if the document is critical to office operations.

B.2.6 Communications: The inventory must fully identify all communications networks (i.e., line identifiers, condition types, speed, types/periods of service, protocols, protection features, connectivity, and vendor). It must also indicate criticality and time frame for each circuit.

B.2.7 Environmental/Utilities Support: The inventory must identify and describe special environmental support equipment, all utilities connectivity to include backup and UPS power, and any special physical security provisions that are critical to essential operations. The description should include technical specifications, identification of vendor, replacement cost/time (if known), and indicate criticality in terms of AIS hardware support requirements.

B.2.8 Furnishings: The inventory must specify the type and quantity of required furnishings. (NOTE: Furnishings should be kept to the absolute minimum in terms of quantity and type.) It must identify replacement vendor(s) and cost/time (if known).

B.2.9 Supplies and Forms: Special IT supplies and forms, as well as a limited quantity of routine office supplies, must be identified in the inventory. The inventory should describe the use of any special supplies and forms, identify the responsible individual, the location of both normal operating stocks and backup supply, description of the item, and vendor or resupplier.

B.2.10 Technical/Maintenance Support: The inventory must identify special technical and maintenance support minimum requirements, identify suppliers, identify and describe existing support agreements, and/or describe procedures and responsible individuals for obtaining needed support.

B.2.11 Personnel: Personnel are not normally listed in the resources inventory except in terms of staffing requirements. In developing a COOP, staffing should be kept to the absolute minimum necessary to perform essential functions. Key individuals are identified by name and assigned duties as part of the continuity of operations team.

Inventory format is at the discretion of the COOP planner. However, it should detail requirements as discussed above and should be inserted into the COOP.

APPENDIX C: CONTINUITY OF OPERATIONS PLAN MODEL

CONTINUITY OF OPERATIONS PLAN (COOP)

FOR

[[[[[[OFFICE NAME]]]]]]

CITY, STATE/ZIP

EXECUTIVE SUMMARY

THE PURPOSE OF THE EXECUTIVE SUMMARY IS TO PROVIDE A BRIEF OVERVIEW OF THE CONTENTS OF THE PLAN AND TO BRING KEY DECISION POINTS TO THE ATTENTION OF THE SENIOR OFFICIAL. ENSURE THAT THESE DECISIONS ARE CLEARLY OUTLINED FOR THE DECISION MAKER WHEN THE DRAFT PLAN IS SUBMITTED FOR APPROVAL. FOLLOWING APPROVAL OF THE DRAFT PLAN, THESE DECISIONS WILL BE STATED AS FACTS.

The objective of this Continuity of Operations Plan (COOP) is to ensure that the [[[[[[OFFICE NAME]]]]]] has sufficient resources to continue essential operations should computer operations be affected by an adverse event such as fire, severe storm, power disturbance/interruption. This objective is accomplished by detailing the preparatory actions necessary to support the COOP and by providing an action plan to be used should an adverse event occur. To reach this objective, the [[[[[[OFFICE NAME]]]]]] Continuity of Operations Plan will identify a team who will be activated during a catastrophic event and will be responsible for ensuring that Information Technology (IT) functions are operational under emergency conditions, until the primary site has become operational or the office relocates to an alternate site, in accordance with the applicable Disaster Recovery Plan.

The following functions and supporting IT systems are critical to the mission of the [[[[[[OFFICE NAME]]]]]]. These functions must become operational within NUMBER OF HOURS after a catastrophic event resulting in the failure of the IT systems or damage to [[[[[[OFFICE NAME]]]]]] office areas:

· INSERT CRITICAL FUNCTIONS/SYSTEMS FROM OFFICE FUNCTION CRITICALITY MATRIX

This COOP has tentatively identified TEMPORARY SITE as the temporary office site. Currently, the [[[[[[OFFICE NAME]]]]]] does not have formal arrangements in place for fulfilling its IT processing and communications requirements at a temporary site. Thus, should a disaster occur which would render the [[[[[[OFFICE NAME]]]]]] primary facility inoperative, the critical functions of the [[[[[[OFFICE NAME]]]]]] would cease, and any chance of a prompt resumption of IT processing activity would be greatly diminished. The following IT systems and general resources are critical to the accomplishment of the [[[[[[OFFICE NAME]]]]]] mission:

- INSERT SELECTED HARDWARE, SOFTWARE/DATABASE, AND COMMUNICATIONS RESOURCES FROM THE CRITICAL RESOURCES INVENTORY

It is recommended that:

· Consideration be given to identifying and formally designating a temporary site with compatible AIS processing and communications systems, and that this site be the TEMPORARY SITE, OFFICE, OPERATING ADMINISTRATION, AGENCY, OR OTHER LOCATION;

· Consideration be given to identifying and formally designating a backup storage facility for the secure storage of critical backup software and database media, supporting documentation and files, and certain critical supplies, and that this site be the IDENTIFY BACKUP STORAGE LOCATION; and

Consideration be given to identifying, designating, and pre-positioning the critical software, databases, documentation, files, and supplies identified in this plan.

Table of Contents

Education and Training

PLAN OVERVIEW

INTRODUCTION

This Continuity Of Operations Plan (COOP) for the [[[[[[OFFICE NAME]]]]]] was developed to assist in preventing events which might disrupt [[[[[[OFFICE NAME]]]]]] business operations and services, where possible, and to minimize the potential impact on the [[[[[[OFFICE NAME]]]]]] of any unavoidable disruption. This Plan recognizes the possibility that individuals may execute resumption and recovery operation with limited prior exposure to or knowledge of the entire plan in detail. Therefore, the plan's development focused on the following issues:

- heightened awareness of management and employees
- advanced preparation to minimize impact potential; and,
- training in the execution of pre-defined and pre-assigned responsibilities and tasks.

The [[[[[[OFFICE NAME]]]]]] COOP includes the strategies, actions, and procedures to resume the business operations and functions located at:

Department of Transportation (DOT)

[[[[[[OFFICE NAME]]]]]]

Office Address

This chapter of the Plan document contains a statement of management policy. It identifies the plan's objectives, its scope and limitations, the assumptions made during its development and guidelines for administering the plan’s contents.

STATEMENT OF POLICY

DOT and [[[[[[OFFICE NAME]]]]]] recognize and acknowledge that the protection of its assets and business operations is a major responsibility to its employees and to the communities it serves. Therefore, it is a policy of DOT and [[[[[[OFFICE NAME]]]]]] that a viable COOP be established and maintained to ensure high levels of service quality and availability. It is also a policy of DOT and [[[[[[OFFICE NAME]]]]]] to protect life, information and equipment, respectively, in that order. To this end, procedures have been developed to support the resumption of time-sensitive business operations and functions in the event of their disruption at [[[[[[OFFICE NAME]]]]]]. [[[[[[OFFICE NAME]]]]]] is committed to supporting service resumption and recovery efforts at alternate facilities, if required. Likewise, [[[[[[OFFICE NAME]]]]]] and its management are responsible for developing and maintaining a viable COOP that conforms to acceptable insurance, regulatory and ethical practices and is consistent with the provisions and direction of DOT strategic and tactical plans.

OBJECTIVES

The objective of a COOP is to assist [[[[[[OFFICE NAME]]]]]] in resuming time-sensitive business

operations and services, its technology, and its support operations in a timely and organized manner to continue as a viable and stable entity.

The primary objectives of this COOP are:

- To provide a tested vehicle which, when executed, will permit and support an efficient, timely resumption of the interrupted business operations.
- To ensure the continuity of the services provided from the affected facility
- To minimize inconvenience and potential disruption to other business functions.
- To minimize the impact to DOT's public image and adverse financial effects of an outage.

This COOP also seeks to minimize the following:

- The number and frequency of 'ad hoc' decisions which must be made following a disaster.
- [[[[[[OFFICE NAME]]]]]]'s dependence on the participation of any specific person or group of persons.
- The need to develop and implement new procedures once the disaster has occurred.
- The loss of data and information, recognizing that some loss is inevitable.
- Confusion and exposure to errors, omissions and unnecessary duplication of effort.
- The total elapsed time to execute response, recovery and restoration processes.

[[[[[[OFFICE NAME]]]]]]

PLAN OBJECTIVES

With these general objectives in mind, the [[[[[[OFFICE NAME]]]]]] COOP has been developed to accomplish the following, specific objectives:

- To resume technology operations and support for time-sensitive DOT business operations in the event existing technology processing has been rendered inoperable at the [[[[[[OFFICE NAME]]]]]].
- To reduce the operational effects of a disaster on DOT time-sensitive business operations through a set of pre-defined and flexible procedures to be used in directing recovery operations.
- To resume production processing of the most time-sensitive [[[[[[OFFICE NAME]]]]]] computer systems, network services and applications within 7 calendar days following the disruptive event.
- To resume production processing of less time-sensitive [[[[[[OFFICE NAME]]]]]] computer systems and applications within 8 to 30 calendar days following the disruptive event.
- To resume full processing capability, including test and development work, for [[[[[[OFFICE NAME]]]]]] technology and operations within 30 to 45 calendar days following the event as permitted by the restoration effort.
- To resume and maintain adequate service levels to DOT customers.
- To provide a proper work environment for displaced staff while the [[[[[[OFFICE NAME]]]]]] and its contents is being restored.
- To ensure that normal [[[[[[OFFICE NAME]]]]]] business operations are restored in a timely manner.
- To provide [[[[[[OFFICE NAME]]]]]] with a viable, well-maintained plan.

SCOPE

The scope of this plan includes time-sensitive and less time-sensitive [[[[[[OFFICE NAME]]]]]] business functions, automated technology, and support areas of [[[[[[OFFICE NAME]]]]]] located at [[[OFFICE LOCATION]]]. This Plan will be activated in the event that the [[[OFFICE LOCATION]]] or a portion of it is involved in an emergency or is declared unusable for normal operation.

This Plan addresses business resumption and recovery in a disaster situation as indicated above. It does not address building emergency and evacuation procedures or on-site resumption and recovery procedures. Actions related to the physical restoration process, in terms of primary site restoration, recovery de-activation, migration and re-establishment of normal operations, termination/shutdown of recovery operations at alternate sites and post-recovery operations are addressed in the tasks of the teams. This Plan was based on DOT management approval of those applications and associated support functions identified as time-sensitive. The time-sensitivity of the applications and services delivered from [[[[[[OFFICE NAME]]]]]] was documented during the pre-planning process known as a business plan analysis. The business plan analysis identified the time-sensitive business operations, automated technology processes, time-sensitive support operations and tolerable outage periods for which and after which disruptions could result in significant losses to DOT. The resulting application recovery priorities on which this plan is based are documented in the report ‘Computing Processes by Criticality’ included in the plan’s appendices.

ASSUMPTIONS

The purpose of this section is to define the assumptions that were made in developing the plan for

[[[[[[OFFICE NAME]]]]]].

Disaster: A disaster is considered to be any event that would render the [[[[[[OFFICE NAME]]]]]] facility unusable or inaccessible for a period of time estimated to exceed 2 business days.

Worst-Case Interruption: [[[[[[OFFICE NAME]]]]]] facilities are totally unusable or inaccessible and there is no salvageable equipment, data, documentation, etc.

Less-Severe Interruption: Although the plan is designed for the worst case, the ability to resume operations from less serious interruptions is inherent within the plan because of the plan’s structure by time-sensitive application, information system and support area.

Localized Emergencies: In circumstances involving a localized event (i.e. limited to

[[[[[[OFFICE NAME]]]]]]), equipment vendors and local utility companies should normally be able to install replacement computer and communications hardware and telephone circuits in 'x' to 'x' calendar days. This assumes that replacement service/equipment orders are placed on an "emergency" basis at the time of the event. It also assumes that [[[[[[OFFICE NAME]]]]]] can quickly obtain and prepare suitable alternate site(s) to serve as an interim or temporary resumption and recovery centers for its business operations and information processing centers, in a period of 3 to 5 days.

Regional Emergencies: In the event of a regional emergency, such as an earthquake or a tornado, the time to acquire the necessary computer equipment and data circuits could require weeks. This will be due to multiple organizations contending for the same emergency resources

and services. Regional emergencies which cause wide-spread disruption of public utilities such as electricity, water and network services may also cause additional delays in re-establishing DOT [[[[[[OFFICE NAME]]]]]] business and technology operations without pre-identified and pre-conditioned/contractual alternate backup sites.

Alternate Operating Sites: This plan assumes that [[[[[[OFFICE NAME]]]]]] will have access to and use of sufficient physical sites within the DOT environment to meet its application recovery time objectives. Sites currently considered eligible [[[[[[OFFICE NAME]]]]]] temporary recovery locations are listed in the report ‘Location Information’ located in the plan appendices. The pre-positioning of redundant equipment, environmental conditioning and access to the DOT WAN necessary to accomplish application recovery is addressed in [Appendix ?]

Plan Documentation: The level of documentation in the plan assumes and requires that [[[[[[OFFICE NAME]]]]]] management and staff are familiar with [[[[[[OFFICE NAME]]]]]] 's business operations, its automated technology and the requirements of the [[[[[[OFFICE NAME]]]]]] COOP.

Available Personnel: Sufficient management and staff, familiar with and trained in the procedures and tasks in this plan, will be available subsequent to the interrupting event t execute their recovery responsibilities and to support the restoration effort. [[[[[[OFFICE NAME]]]]]] personnel understand that, following a major interruption of services/operations, it will not be a matter of "business as usual" but "survival".

Vital Records: All business documentation, files that would be necessary for resumption and recovery purposes are backed up and stored/located safely away from the [[[[[[OFFICE NAME]]]]]] using a rotation schedule that minimizes data loss.

[[[[[[OFFICE NAME]]]]]] Computer Data: All computer files required to implement resumption of the [[[[[[OFFICE NAME]]]]]] current operating environments, and/or that support time-sensitive business operations are backed up daily. This information is rotated to a safe offsite location according to a schedule that minimizes data loss and the effort to reconstruct production environments. The type of backups and the timing of the off-site rotation and retention are approved by DIT management and are considered sufficient to minimize the re-entry/re-construction of data and the recreation/forward recovery of files to current status.

Backup Storage Locations: All backup items for resumption and recovery are stored on-site and off-site or can be easily and quickly obtained or created from other identified sources. The backups stored on-site are in a series of fire resistant safes that are located within the [[[[[[OFFICE NAME]]]]]] data center boundaries. The backups stored off-site are in a secured location that is sufficiently distant from the primary site so they will be unaffected by most interrupting events. These stored backups are considered to be the only resources available to implement resumption. This plan assumes that the locations (other than the [[[[[[OFFICE NAME]]]]]]) where backups are stored were not affected by the emergency incident/situation and can be accessed by DOT personnel.

Internal and External Contacts: All information necessary to complete the internal and external contacts quickly and accurately during resumption is documented and maintained in the plan.

Application Recovery Time Frames: The time frame in which each time-sensitive application and supporting computer/network system has been set by DOT [[[[[[OFFICE NAME]]]]]] Management, is current with the needs of [[[[[[OFFICE NAME]]]]]]’s clients and is available within this plan. The resumption of each application is greatly dependent on the availability of [[[[[[OFFICE NAME]]]]]] personnel, its information files, and its access to the IT systems and data files. Actual time-frames for resumption and recovery may be influenced by the availability of alternate operating sites,

hardware and software, current backup files, and the reload time requirements of the IT System architectures.

RECOVERY STRATEGY

Loss of functionality at [[[[[[OFFICE NAME]]]]]] will have a significant impact on application and data delivery throughout DOT. The [[[[[[OFFICE NAME]]]]]] COOP has been developed to respond effectively to a significant outage by using a pre-defined method for utilizing various facility, staff and technical resources. This method, known as the recovery strategy, has been selected to help ensure that [[[[[[OFFICE NAME]]]]]] will accomplish the resumption and recovery of business functions within stated time frames at required levels of service. Serous consideration has been given to selecting a recovery strategy that is workable as well as cost efficient. This Plan's recovery strategy anticipates the availability of other DOT/Federal Agency locations for use as alternate processing and network termination sites. (A prioritized list of eligible locations is provided in the 'Location Information' report in the Action Plan section of this document.) The sites were selected for their ability to support the [[[[[[OFFICE NAME]]]]]]'s technical infrastructure requirements while providing the best possible access to the DOT WAN. Selected [[[[[[OFFICE NAME]]]]]] continuity teams will relocate to the selected sites and begin preparing them for use as alternate processing locations should a business disruption require the activation of this plan. Where pre-positioned equipment and services are in place, [[[[[[OFFICE NAME]]]]]] teams will activate those resources as soon as possible. Where additional equipment and other services are needed to upgrade a site to full utilization, these items will be acquired and installed on an emergency basis. Configuration details for current [[[[[[OFFICE NAME]]]]]] Nodes, Servers and network management device are included in this plan to help expedite this "acquire time of disaster" strategy as are the current inventory of DOT contracts for which emergency requisitions will be drafted (see Action Plan Appendices).

PLAN ADMINISTRATION

The scope of administration duties and responsibilities includes, but is not limited to, the continued endorsement of the plan through the mandatory, documented review of the plan by [[[[[[OFFICE NAME]]]]]] management and team members, on no less than an annual basis. A report on the plan's administration is to be presented/submitted to DOT Sr. Management annually or as otherwise required. The [[[[[[OFFICE NAME]]]]]] ISSO is responsible for the administration of the plan. The ISSO will ensure that DOT and [[[[[[OFFICE NAME]]]]]] standards and procedures are developed to address plan administration needs. The ISSO will also include any relevant, related documentation in the Plan. As custodian and administrator of the [[[[[[OFFICE NAME]]]]]] COOP, the ISSO must have a thorough knowledge of all Plan contents. As a further safeguard, the ISSO should never be the sole person in the organization with extensive knowledge of the structure and contents of the Plan; an alternate COOP Coordinator should be a full participant in all Plan maintenance and exercise activities. Responsibility for maintaining specific sections of the [[[[[[OFFICE NAME]]]]]] COOP resides with each Team Leader in accordance with the Team's objectives and functional responsibilities for Response, Resumption, Recovery and Restoration. Team Leaders must ensure compliance with these documented procedures for Plan administration. Each [[[[[[OFFICE NAME]]]]]] employee, regardless of their role as a team member, is responsible for providing updated personal contact information to the ISSO as changes occur.

Each [[[[[[OFFICE NAME]]]]]] employee is responsible for the maintenance of [[[[[[OFFICE NAME]]]]]]'s capability to respond and resume operation following a disaster. Some individuals will have more direct responsibility than others will. Nevertheless, each individual must be aware of the necessity for the preservation of such a continuity capability and must perform to the utmost to ensure that the response, resumption, recovery or restoration capability is truly viable. Should a plan review necessitate changes or updates, the ISSO is responsible for implementing the changes and issuing updated Plan documentation. Individuals in responsible management

positions will be called upon periodically to provide information necessary for maintaining a viable plan and an exercised continuity capability.

CONTINUITY PROCESS OVERVIEW

INTRODUCTION

This section outlines the four major stages of the continuity process as it applies to this plan. It

describes the central activities and objectives of each stage and the relationships among stages. Actual circumstances of the business interruption or disaster will determine whether a particular stage is initiated and how long it will take to complete. This section provides guidelines and explains continuity process. The information needed to implement each stage is located in the Action Plan section of this document.

EMERGENCY RESPONSE

Following the notification of the emergency incident or situation, a team of key [[[[[[OFFICE NAME]]]]]] personnel, the Assessment team, will first assemble at the incident site and immediately begin to

assess and evaluate the altered business environment for DOT [[[[[[OFFICE NAME]]]]]].

The primary objectives of the [[[[[[OFFICE NAME]]]]]] Assessment team are:

1. To establish an immediate and controlled DOT presence at the incident site;
2. To conduct a preliminary assessment of incident impact, known injuries, extent of damage, and disruption to the [[[[[[OFFICE NAME]]]]]]'s services and business operations;
3. To notify the [[[OFFICE NAME]]] Management team;
4. To determine if and/or when access to the [[[OFFICE NAME]]] facilities will be allowed; and
5. To provide the [[[OFFICE NAME]]] Management team with the facts necessary to make informed decisions regarding subsequent recovery activity.

It must be noted that response to an emergency does not necessarily or automatically translate into the declaration of a disaster and the implementation of a full resumption operation.

Activation of the [[[OFFICE NAME]]] disaster recovery portion of the COOP requires significant expenditures of time, personnel and financial resources. The [[[OFFICE NAME]]] Management team will determine whether or not the expenditure of resources are warranted and to what extent they are justified based on the information and recommendations provided by the Assessment Team. Refer to the Action Plan portion of this document for contact lists, team assignments, and checklists of specific tasks to be performed. The flowchart on the following page provides a graphical overview of the Emergency Response process.

Figure 1: Emergency Response Process

INCIDENT ALERT

Initial notification of an incident or situation is expected to come directly from a [[[OFFICE NAME]]] staff member. Other potential sources of incident notification might be the police, the fire company, security service, the news media, etc. In any case, if you are the first employee to become aware of an emergency situation at the [[[OFFICE NAME]]], it is important that you contact the members of the [[[OFFICE NAME]]] Assessment team about the emergency incident as soon as possible. They will begin emergency response activities and alert the [[[OFFICE NAME]]] Management team. Initial attempts to contact the [[[OFFICE NAME]]] Management teams should not exceed two hours. After that time, the Assessment Team leader should list the names of individuals could not be contacted and assign someone else to continue the notification process and/or to temporarily assume the individuals assigned responsibilities.

SAMPLE INCIDENT ALERT SCRIPT

The following format is suggested for all individuals receiving/providing notification of an emergency incident or situation:

1. If you receive a call notifying you of an emergency incident or situation, write down the message. Repeat the message back to the caller to verify its accuracy.
2. Request that the individual making the notification meet the [[[OFFICE NAME]]] Assessment Team at the incident site. Provide an estimated time of arrival.
3. If you are the first person notified, contact [[[OFFICE NAME]]] Facilities Management to verify the reported emergency incident or notification.
4. Notify the [[[OFFICE NAME]]] Assessment Team. Refer to the Action Plan for contact information.
5. Read the information received to each person you call, briefly stating the nature of the problem and the time of the reported incident. Do not speculate on injuries or damage to avoid possible confusion.
6. Instruct each person you contact to proceed to the pre-determined emergency meeting site or other designated location. Determine each person's estimated time of arrival.
7. Instruct all individuals contacted to avoid making comments to news media, customers, vendors, etc. An official DOT-designated spokesperson will provide the news releases to the press, news media, etc.
8. Give instructions to each contacted individual as to what is expected of them, (e.g. report to the emergency response site, stand by for further instructions, etc.). Activate only the employees needed immediately and prepare a notification list and contact schedule for other individuals if required.
9. Maintain a record of all calls attempted and completed. Report the notification results to the WWC Management Team

NOTIFICATION GUIDELINES

All Team Leaders and Team Members have been assigned call tree responsibilities that should

be followed during the emergency notification. The [[[OFFICE NAME]]] Management Team will determine if DOT sites with time-sensitive functions should be notified and a disaster situation declared based on the preliminary assessment of the situation. If the emergency notification procedures are initiated, each Team Leader will be responsible for contacting their Alternate Team Leader and Team Members with specific instructions. If the Team Leader is not available, the Alternate Team Leader will assume the Team Leader’s responsibilities. In the event the Alternate Team Leader is also not available, the [[[OFFICE NAME]]] Management Team will assign someone to complete the notifications until the Primary or Alternate Team Leaders

become available and resume their responsibilities. It is important that all key personnel be notified of the disaster as soon as possible to begin business resumption operations. The Employee/Contractor Notification List has the telephone numbers for the essential personnel to be notified in predetermined sequence.

OBJECTIVES

The objectives for the continuity organization during emergency response are as follows:

1. Complete emergency response, notification and mobilization duties as directed by the [[[OFFICE NAME]]] Management Team.
2. Ensure the [[[OFFICE NAME]]] Management Team is contacted and appraised of situation's status and activity.
3. Obtain reports of personnel injury or related matters from Facilities or Security and/or local authorities.
4. Perform assessment(s) and evaluation(s) until the extent of impact or damage can be determined.
5. Document the results of the preliminary assessment(s) and evaluation(s) and submit the report to the [[[OFFICE NAME]]] Management Team with recommendations to terminate the emergency response activities or activate subsequent plan operations.
6. Terminate or expand/extend the operation as directed by the [[[OFFICE NAME]]] Management team.

RESUMPTION

During the Resumption stage of the continuity process, [[[OFFICE NAME]]] will use its pre-defined alternate sites to reestablish processing and network capability for the most time sensitive DOT applications. The [[[OFFICE NAME]]] Management Team will initiate this plan if they determine that the interruption is significant enough to warrant its activation. Note that resumption activities may be executed concurrently with emergency response actions.

Key elements of the resumption phase include:

- Establishing and organization a Command Center from which to manage resumption activities.
- Activating and mobilizing the continuity teams needed resume time-sensitive application restoration.
- Evaluating alternate site equipment and network service for the necessary enhancements to support time-sensitive application recovery.
- Mobilizing and activating the support teams needed to support enhancement and use of the alternate site(s).
- Notifying and informing [[[OFFICE NAME]]] clients and DOT Management of the situation.
- Alerting employees and close contractors not assigned to the continuity organization, vendors and other key organizations to the situation and the their role during resumption and recovery.

Once mobilized, the Support teams will be instructed in their reporting and action requirements. The necessary site assessments, evaluations and the initiation of salvage operations will be completed once the Command Center is established. Additional alerts to supporting vendors, management and customers will also be conducted from the Command Center.

Based on the information/recommendations provided by the [[[OFFICE NAME]]] Assessment & Salvage team, the [[[OFFICE NAME]]] Management team will determine whether or not the expenditure of the above resources are warranted, to what extent they are justified, and what actions will be taken.

OBJECTIVES

The objectives that will become the major focus of the Resumption stage are:

- To prepare for and/or implement the procedures necessary to facilitate and support the resumption process and subsequent restoration operations, as required.
- To mobilize and activate the continuity teams responsible for reactivating critical applications.
- To alert employees, vendors and other internal and external individuals and organizations.
- To begin implementing procedures to re-establish time-sensitive processes and applications. This may include relocating to a temporary facility, re-establishing communications at an alternate site, etc.

COMMAND CENTER

A Command Center headquarters will be established if management decides to continue and escalate situation from emergency response to resumption operations. The site for the Command Center headquarters site should be identified in advance. Initial activities performed at the Command Center are described below:

- If the [[[OFFICE NAME]]] facility can be accessed, further assessments and evaluations of the on-site conditions, the damage impact and extent of the emergency incident/situation will be completed.
- Use of the command center may be confined to management meetings and the cancellation of the resumption operation if the facility (e.g., work areas, fixed assets, files, equipment, voice communications, etc.) are unaffected and the emergency incident/situation problems can be resolved without major impact to service delivery.
- If the information about the emergency incident/situation problems is inconclusive, the command center will be used as a meeting site until the assessments are completed.
- If the emergency incident/situation is such that the resumption operation needs to be continued or further escalated, and/or a disaster declared, the command center should be organized and the appropriate support and resumption teams notified and activated as required.

RECOVERY

The Recovery stage of the continuity process concerns the re-activation of a greater scope of business processes and services beyond the most time-sensitive processes. [[[OFFICE NAME]]] Management will initiate recovery stage operations if the estimate of total outage indicate the need to expand service delivery using alternative locations and resources. If, for example, the impact on the [[[OFFICE NAME]]] facility is expected to take more than 30 days to resolve, the recovery stage may be initiated at alternative sites and the appropriate resources devoted to those applications. Alternatively, if it is estimated that 15 days would be needed to restore [[[OFFICE NAME]]] to full function, [[[OFFICE NAME]]] Management might initiate a parallel effort to resume less time-sensitive operations at [[[OFFICE NAME]]], while planning the migration of resumption activities from the alternate site to the [[[OFFICE NAME]]] facility. Consequently, recovery, resumption and restoration stage activities may be conducted with some parallelism as dictated by the situation.

OBJECTIVES

The objectives for recovery stage operations include:

- Maintaining a Command Center, which provides sufficient support for resumption and recovery operations.
- Mobilizing and activating additional continuity teams to facilitate the recovery of less time-sensitive business operations.
- Maintaining an adequate level of Support team coverage to support all business operations.
- Maintaining an adequate level of technology team coverage to sustain information processing service demand as they grow in scope.
- Maintaining communication with the continuity organization, clients and senior management.

COMMAND CENTER

The level of support maintained at the Command Center headquarters during recovery will be determined by the [[[OFFICE NAME]]] Management team based upon:

- the scope of the disaster,
- the number of business operations and/or applications affected,
- the level of support required for the recovery of business operations; and
- the perception of on-going risks and/or exposures.

RESTORATION

When local officials allow access to the building, the [[[OFFICE NAME]]] Management team will initiate the Restoration phase of this plan. The Restoration stage builds on the assessments performed in the emergency response stage with the goal of returning the impacted facility to its pre-disaster capabilities. In circumstances where the original facility was assessed as beyond repair, this stage will involve the acquisition and outfitting of new permanent facilities.

The restoration process will include the assessment of:

- environmental contamination of the affected areas;
- structural integrity of the building; and
- the damage to furniture, fixtures and equipment.

Restoration will begin in earnest when solid estimates of contamination, structural damage and asset loss can be obtained and personnel resources can be dedicated to the management and coordination of the process. This phase may be executed sequential to, or concurrent with, the Resumption and/ or Recovery stages.

OBJECTIVES

In addition to maintaining a Command Center that provides sufficient support for resumption and restoration operations, objectives of the Restoration stage are to:

- maintain an adequate level of support team coverage to support all business operations,
- maintain an adequate technology teams coverage to sustain information processing operations,

- maintain communication with the continuity organization,
- clean and/or decontamination of the building,
- repair and/or restore the building or construct/acquire of a new facility,
- replace the contents of the building and,
- coordinate the relocation and/or migration of business operations, support and technology departments from temporary facilities to the repaired or new facility.

CONTINUITY TEAM ORGANIZATION

OVERVIEW

In the event of a disaster, the normal organization of DOT [[[OFFICE NAME]]] will shift to that of the continuity organization. Department will shift from the current organizational, "business as usual", structure to an organization working towards survival and the resumption of time-sensitive business operations. The teams associated with this plan represent [[[OFFICE NAME]]] functional units and/or or support functions developed to respond, resume, recover or restore operations of the [[[OFFICE NAME]]] facility. Each team is comprised of individuals with specific responsibilities or tasks that must be completed to fully execute the plan. A primary and alternate team leader who is responsible to the plan owner leads each team. Each team is a sub-unit of the continuity organization. Each team is structured to provide dedicated, focused support, in the areas of its particular experience and expertise, for specific response, resumption and recovery tasks, responsibilities, and objectives. A high degree of interaction among all teams will be required to execute this plan. Each team's eventual goal is the resumption/recovery and the return to stable and normal business operations and technology environments. Each team leader will report status and progress updates its management team throughout the continuity process. Close coordination must be maintained with [[[OFFICE NAME]]] Management and each of the other teams throughout the resumption and recovery operations.

The primary responsibilities of the continuity organization are:

- To protect employees and information assets until normal business operations are resumed.
- To ensure that a viable capability exists to respond to an incident.
- To manage all response, resumption, recovery and restoration activities.
- To support and communicate with DOT staff and other locations within the enterprise.
- To accomplish rapid and efficient resumption of time-sensitive technology and business operations.
- To ensure all insurance and regulatory requirements are satisfied.
- To exercise impact resumption and recovery expenditure decisions.
- To streamline the reporting of resumption and recovery progress between the teams and both [[[OFFICE NAME]]] and DOT Management.

During Emergency Response, the primary responsibilities of the continuity organization are:

- To establish an immediate and controlled company presence at the incident site
- To conduct a preliminary assessment of incident impact, known injuries, extent of damage, and disruption to the enterprise’s services and business operations.
- To determine if and/or when access to the Wilton Woods facility will be allowed.
- To provide Executive Management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity.

During Resumption, the primary responsibilities of the continuity organization are:

- To establish and organize a control center for the resumption operations.
- To notify and appraise team leaders of the situation.
- To mobilize and activate the operations teams necessary to facilitate the resumption process;
- To alert employees, vendors and other internal and external individuals and organizations.

During Recovery, the primary responsibilities of the continuity organization are:

- To prepare for and/or implement procedures to facilitate and support the recovery of less time-sensitive business operations.
- To mobilize additional continuity teams and support organizations as required.
- To maintain an information flow regarding the status of recovery operations among employees, vendors and other internal and external individuals and organizations.

During Restoration, the primary responsibilities of the continuity organization are:

- To manage salvage, repair and/or refurbishment efforts at the affected facility.
- To prepare procedures necessary to the relocation or migration of business operations to the new or repaired facility.
- To implement procedures necessary to mobilize operations, support and technology department relocation or migration.
- To manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during and after relocation or migration.

ACTIVATION OF THE PLAN

Activation of FCPS DIT plan will be executed when an emergency occurs that necessitates a response beyond the scope of standard daily operating procedures. Only the following selected personnel may activate this entire plan, or any phase thereof, and/or declare a disaster situation for DOT [[[OFFICE NAME]]]. The [[[OFFICE NAME]]] Management team will decide whether or not to activate the Plan and/or declare a disaster. Their decision will be based on a preliminary assessment of the business interruption incident, including any physical impairment to the facility. Pending their decision, emergency notification of DOT [[[OFFICE NAME]]] personnel will be initiated and the entire plan, or any phase thereof, will be activated, as directed.

- Technology teams focused on restoring data center based applications will be activated only as directed by the [[[OFFICE NAME]]] Management team. Each team consists of unique procedures, tasks, contact and resource information. Applications will be restored according to established priorities.
- [[[OFFICE NAME]]] unit restoration teams will be activated only as directed by the [[[OFFICE NAME]]] Continuity Management team based on the impact of the disruption. Business unit restoration priorities will be established in response to the disruption. Business unit staff will focus on supporting data center and application recovery priorities. Team procedures, resources and procedures are included along with specific business unit attachments (e.g. resource and notification information) and action tasks.

TEAM ROLES AND RESPONSIBILITIES

Following the Response phase of the plan, [[[OFFICE NAME]]] has organized into teams to execute its resumption and recovery activities on behalf of DOT. To accomplish the tasks

assigned, each team will draw upon the expertise of supporting organizations both internal and external, as necessary. This section of the plan identifies the major groups of teams required to accomplish recovery. Each team has a minimum of a leader and one or more members representing the skills appropriate to the team's role. Team leaders/alternates must be thoroughly familiar with the responsibilities not only of their team, but also of all the teams with which they must interact. A detailed list of teams and their current team members are located in the Action Plan.

The roles and responsibilities of each major group of teams are outlined below.

[[[OFFICE NAME]]] MANAGEMENT

- Approve the activation of the plan or the declaration of a disaster.
- Approve expenditures as required.
- Coordinate with DOT Management on the issuance of related news releases to the press and media.
- Monitor all activities with the Recovery and Restoration Management teams.
- Provide executive management direction and counsel to activated teams as required.
- Coordinate all personnel matters and issues involving employee fatalities and injuries and notifications to employees' families and dependents with DOT management. This may also include professional counseling and financial support for employees.
- Review progress and status with DOT Management.
- Manage the resumption and recovery of all [[[OFFICE NAME]]] business operations and service delivery.
- Establish and organize a business resumption headquarters at an alternate site. Organize the business resumption Command Center.
- Direct and support team leaders. Make assignments, as appropriate.
- Ensure that a damage assessment and salvage operation is conducted at the primary site.
- Control the activation of the business resumption procedures.
- Coordinate the eventual restoration/relocation of the primary site.
- Report resumption and recovery progress to DOT Management.

DATA CENTER RECOVERY MANAGEMENT

- Contact key personnel required for resumption of time-sensitive functions. Alert all personnel and instruct them to report to their designated areas, as required.
- Perform tasks to resume time-sensitive functions, as required.
- Work with support teams to obtain support required for service delivery.
- Report the status of resumption activity to the [[[OFFICE NAME]]] Management team.
- Manage all administrative activities associated with the resumption and recovery operations.
- Notify alternate backup sites and/or vendors of disaster declaration.
- Identify and coordinate procurement for equipment and services for alternate site installation.
- Identify and retrieve all backup files from off-site storage.
- Request assistance to establish data and telecommunications if necessary.
- Execute IT Systems resumption procedures.
- Manage IT Systems operations at the alternate and primary sites if necessary.

[[[OFFICE NAME]]] RESTORATION MANAGEMENT

- Coordinate salvage and/or reconstruction of the [[[OFFICE NAME]]] facility if appropriate.

- Coordinate the acquisition and outfitting of a new permanent site if necessary
- Identify and coordinate procurement for equipment and services for the permanent site.
- Work with DOT support teams to obtain required services to restore and outfit a permanent [[[OFFICE NAME]]] data center and office location.
- Manage preparation of a migration plan from the alternate site to the permanent site.
- Coordinate migration and move-in logistics with the [[[OFFICE NAME]]] Management, Data Center Recovery teams and with DOT support services.

REPORTING STRUCTURE

The following chart is a graphic representation of the reporting structure for the [[[OFFICE NAME]]] continuity organization that reflects the overall team organization and reporting structure that will be employed during response, resumption, recovery and restoration processes.

[INSERT [[[OFFICE NAME]]] CONTINUITY ORGANIZATION HERE]

PLAN MAINTENANCE

INTRODUCTION

COOP maintenance procedures are divided into two general categories: scheduled and unscheduled. Scheduled maintenance is time-driven, where unscheduled maintenance is event-driven.

SCHEDULED MAINTENANCE

Scheduled maintenance consists of quarterly reviews and updates as well as annual structured walk-through and/or tactical exercises (as described in the Plan Exercise section of this document). The purpose of the plan review is to determine whether changes are required to procedures, the continuity organization, and notification procedures. The ISSO is responsible for initiating scheduled maintenance activities in consultation with the [[[OFFICE NAME]]] Management Team. The ISSO shall initiate quarterly continuity plan reviews in the X week of the Y month of each quarter. He/she shall notify all continuity organization team leaders and alternate team leaders to review the response, resumption, recovery and restoration task lists, contact information and procedures for changes that may be required. Other DIT staff members may be invited to satisfy the needs of a specific review session. The reviews address events that have occurred within each team's area of responsibility that may affect the response, resumption, recovery and restoration capability. Teams shall submit required changes to the ISSO not later than the end of the X week of the Y month of each quarter. The ISSO shall incorporate all changes to the plan, distribute updated copies of the plan.

UNSCHEDULED MAINTENANCE

Certain maintenance requirements are unpredictable. The majority of unscheduled changes occur as the result of major changes to service level agreements, hardware configurations, networks, production processing, etc.

Examples of items that may trigger the need for unscheduled maintenance include:

- Changes in data processing architectures, hardware, or environmental changes
- Major changes in operating system(s) or utility software programs
- Major changes in the design of a production database
- Major changes in communications, systems network design or implementation

- Changes in off-site storage facilities and methods of cycling items, etc.
- Improvements or physical changes to the current computer center structure
- Changes in the business or operating environment
- Enterprise organizational changes that effect the continuity teams
- New application systems development
- Discontinuation of an application systems from processing schedules
- Transfers, promotions or resignations of individuals on the emergency notification list or continuity organization teams
- Significant modification of basic functions, data flow requirements, or accounting requirements within an application system

The ISSO must be made aware of all changes to the COOP resulting from unscheduled maintenance. The ISSO shall then notify all continuity organization team leaders and alternate team leaders to review the plan for changes that may be required as a result of the item that has triggered the review. Team leaders will submit actual change data to the ISSO. The ISSO will team up with the person submitting the change and either update the COOP or assign the update responsibility to the affected continuity team(s). Cross-team coordination should be completed within two weeks of the review. Once this is done, the ISSO is responsible for any required updates to the plan, which result from the review. The ISSO shall print hard copies of the plan, and distribute copies.

RESUMPTION AND RECOVERY CONFIGURATION

The Continuity Plan maintenance process should include a periodic re-evaluation of the minimum hardware capacity required to provide short-term response, resumption, recovery and restoration capability. The re-evaluation process must address the capacity growth requirements associated with the increase of transaction processing volumes of the production application systems, as well as the addition of new systems to the production environment. Based on the existing configuration and requirements, it is assumed that the most effective configuration for supporting long-term recovery and restoration will be the installation of the computer hardware required to support normal or near-normal levels of processing in a temporary computer center. Special attention must be paid to ensure continuing compatibility of existing equipment with that which is installed at the alternate site.

PLAN EXERCISE

INTRODUCTION

Documentation and periodic reviews of the [[[OFFICE NAME]]] Continuity Plan are reassuring. However, proof and confidence that the plan will work only results from completion of a successful exercise of the tactical strategies and procedures. Exercises of the [[[OFFICE NAME]]] Continuity Plan are designed to determine:

- The state of readiness of the continuity organization to respond to and cope with a disaster involving the data processing resources.
- Whether backed up data and documentation stored off-site are adequate to support the resumption business operations
- Whether the inventories, tasks, and procedures are adequate to support the resumption of business operations
- Whether the WWC Continuity Plan has been properly maintained and updated to reflect the actual resumption, recovery and restoration needs

TYPE AND SCOPE OF EXERCISES

A comprehensive program of exercises varying in scope and level of detail will help ensure the effectiveness of the [[[OFFICE NAME]]] Continuity Plan. Examples of the types of exercises that may be incorporated in [[[OFFICE NAME]]]'s exercise program are outlined below.

Structured Walk-Through

In the Structured Walk-through, a disaster scenario is established, and the teams "walk-through" their assigned tasks. This is a role-playing activity that requires the participation of at least the team leaders and their alternates. The scenario will be made available in advance of the exercise to allow team members to review their assigned tasks in response to the exercise scenario.

During the Structured Walk-through, the WWC Continuity Plan is checked for any errors or omissions. At the end of the Structured Walk-through any changes to the plan that are found to be necessary are implemented.

Tactical

A Tactical Exercise is a simulated exercise, conducted in a "war game" format. All members of the continuity organization are required to participate and perform their tasks and procedures under announced or surprise conditions. The exercise monitor provides information throughout the exercise to simulate events following an actual disaster. Generally, a disaster scenario is established and provided to all the business continuity team leaders, alternate team leaders, and team members located in a large conference room or utilizing video-conferencing. Each team executes its exercise objectives and interacts with other teams as they complete their actions.

A "speeded up" clock is usually employed in order to complete three days' actions in one working day and requires the teams to respond to the scenario information in near real time.

An eight-hour exercise will usually simulate forty-eight to seventy-two hours of resumption activity. As in the Structured Walk-through, the plan is checked for any errors or omissions. At the end of the Tactical Exercise, any changes to the plan that are found to be necessary are implemented.

Live Production

In a Live Production application system exercise, an operating system is brought to live status on the alternate processor(s), and the data communications network is switched to the alternate site. All resources, other than the computer and communications hardware needed to support this exercise, must be retrieved from the off-site storage facility. This exercise continues to validate the switching capability of the data communications network, and then to the production processing of selected applications systems, including User Login and application system data currency checks. A Live Production exercise will normally be conducted on a weekend when there is a lesser requirement to provide continued service to the user community. Assurance of overall recoverability can only be achieved through the conduct of a complete Live Production Application System Exercise. A Live Production exercise should be conducted once a year as the final exercise of resumption and recovery capability.

Simulation

This type of exercise requires the execution of notification, operating procedures, the use of equipment hardware/software, possible use of alternate site(s), and operations to ensure proper performance. Simulation exercises can and may be used in conjunction with checklist exercises for identification of required plan modification and staff training. Examples of procedures verified

during a simulation exercise include Emergency Procedures, Use of Alternative Methods, Telecommunications Backups, Agent/Vendor/Customer Notifications, Hardware Capacity and Performance, Software Transportability, Alternate Site Access, Team Mobilization, Off-Site File and Information Retrieval, Input Data Retrieval, etc.

Announced And Unannounced

Announced exercises are scheduled exercises generally involving actual resumption of computer processing at the alternate computer facility. Production processing is usually not interrupted, but may be planned for actual resumption and validation at the "Hot Site." This type of test usually involves the entire continuity organization, including selected users along with operations and technical staff.

Unannounced exercises are surprise technical exercises that require processing to be actually recovered at the alternate site. Production processing continues in parallel and is not interrupted. This type of test generally involves only a small portion of the continuity organization and few, if any, users.

When to Exercise

Exercises should be conducted when:

- a major revision to the plan has been completed;
- additional production systems are implemented;
- when significant changes in systems, applications and/or data communications has occurred; and
- the preparedness level of continuity teams must be verified.

Responsibility for Establishing Exercise Scenarios

The ISSO is responsible for making plan exercise recommendations to the [[[OFFICE NAME]]] Management Team and/or enterprise business continuity officials. Such recommendations include rationale for the exercise, the benefits expected to be derived from the exercise, and the specific objectives to be accomplished. A strategy will be developed for each exercise. Development of procedures that measure the effectiveness of the [[[OFFICE NAME]]] Continuity Plan will address the following plan elements:

- Notification
- Organization
- Resources
- Operations

For all exercises, each major plan element may be evaluated independently, or these elements may be exercised as integral parts of the overall plan.

Exercise Scenarios

Exercise scenarios are normally developed to accomplish the objectives established by Executive Management. Some considerations in developing exercise scenarios include:

- Re-exercising the plan segments that were determined to be deficient in past exercises.
- Exercising time-sensitive application systems that have never been recovered or restored, or have not been recently exercised.
- Involving those continuity organization team members that need more training and preparation to maintain familiarity with their functions.
- Ensuring that each exercise involves the use of only off-site storage and inventory items to ensure the completeness and accuracy of the off-site inventory.
- Deciding whether the exercise and associated parameters will be openly announced or will be a surprise. This decision is usually made at the discretion of the enterprise business continuity officials.

Exercise Evaluation

An unbiased evaluation team should evaluate the results of each exercise. This team should be made up of [[[OFFICE NAME]]] or external personnel (such as external auditors) who are removed from any participation in the exercise. The evaluation team should be focused entirely on the validity, currency and capability of the plan to recover and restore DOT time-sensitive application systems at the alternate computing facility.

The Exercise Evaluation Team is charged with the following responsibilities:

- Familiarization with the overall [[[OFFICE NAME]]] Continuity Plan.
- Understanding thoroughly the objectives of the exercise to be conducted.
- Monitoring and observing all the activities of the teams involved in the exercise.
- Ensuring that exercise objectives are met, from the [[[OFFICE NAME]]] and client points of view.
- Documenting findings related to the strengths and weaknesses observed during the exercise.

Each member of the continuity organization that participates in the exercise (team leader, alternate team leader, and team members) will be asked to evaluate the exercise's effectiveness, success and value.

Reviewing Exercise Results

Team leaders and the ISSO will document exercise results as soon as possible, but not later than two weeks after completion of an announced or unannounced exercise. Selected members of the business continuity organization will review exercise results and resolve weaknesses and problems. The ISSO will chair the review and coordinate appropriate changes/updates to the plan. The results of the review will be presented to [[[OFFICE NAME]]] Management and the enterprise business continuity officials.

Schedule of Exercises

The [[[OFFICE NAME]]] Management team will schedule exercises. Exercises will be scheduled with consideration to seasonal production and business cycles, the number of processing systems or platforms in production and the time required to exercise both time-sensitive processes and full production systems.

Education and Training

Awareness of the need for and the process of maintaining a viable continuity capability are essential. This awareness is achieved through formal education and training sessions conducted

on a regular basis. This provides a way of ensuring that the necessary understanding of the business continuity program and processes are understood by the personnel responsible for maintaining and executing the plan.

The objectives of [[[OFFICE NAME]]] Continuity Plan training are to:

- Train the key employees and management who are required to help maintain the plan in a constant state of readiness
- Train the key employees and management who are required to execute various plan segments in the event of an extended computer outage
- Heighten planning awareness for those employees not directly involved in maintaining and/or executing the plan

The ISSO will schedule Educational seminars addressing business continuity in general and the [[[OFFICE NAME]]] Continuity Plan in particular on a regular basis. These seminars will include overviews of the:

- Continuity strategy, priorities and time frames.
- Business continuity organization structure and responsibilities.
- [[[OFFICE NAME]]] COOP structure and contents.
- Data Preservation methodologies and practices.
- Plan administration, maintenance, and exercises.

Top of Page
Back to DIRMM