HNF-5392
Revision 1

Hanford Year 2000 Business Continuity Plan, November, 1999

Prepared for the U.S. Department of Energy
Office of Economic Impact and Diversity

Project Hanford Management Contractor for the
U.S. Department of Energy under Contract DE-AC06-96RL13200

FLUOR DANIEL HANFORD, INC.

P.O. Box 1000
Richland, Washington

INFORMATION CLEARANCE FORM

A. Information Category ☐ Abstract ☐ Journal Article ☐ Summary ☐ Internet ☐ Visual Aid ☐ Software ☐ Full Paper ☐ Report ☒ Other <u>Guidelines</u>		B. Document Number HNF-5392, <u>Rev. 1</u> C. Title Hanford Year 2000 Business Continuity Plan Rev.1 D. Internet Address	
E. Required Information 1. Is document potentially Classified? ☒ No ☐ Yes (MANDATORY) <u>See below for signature</u> <u>12-9-99</u> Manager's Signature Required If Yes _____ ☒ No ☐ Yes Classified ADC Signature Required 2. Internal Review Required? ☒ No ☐ Yes If Yes, Document Signatures Below Counsel _____ Program _____ 3. References in the Information are Applied Technology ☒ No ☐ Yes Export Controlled Information ☒ No ☐ Yes		4. Does Information Contain the Following: (MANDATORY) a. New or Novel (Patentable) Subject Matter? ☒ No ☐ Yes If "Yes", Disclosure No.: _____ b. Information Received in Confidence, Such as Proprietary and/or Inventions? ☒ No ☐ Yes If "Yes", Affix Appropriate Legends/Notices. c. Copyrights? ☒ No ☐ Yes If "Yes", Attach Permission. d. Trademarks? ☒ No ☐ Yes If "Yes", Identify in Document. 5. Is Information requiring submission to OSTI? ☒ No ☐ Yes If Yes UC- _____ and B&R- _____ 6. Release Level? ☒ Public ☐ Limited 7. Charge Code <u>HMFDP191</u> <u>019</u>	
F. Complete for a Journal Article			
1. Title of Journal _____			
G. Complete for a Presentation			
1. Title for Conference or Meeting _____ 2. Group Sponsoring _____ 3. Date of Conference _____ 4. City/State _____ 5. Will Information be Published in Proceedings? ☐ No ☐ Yes 6. Will Material be Handed Out? ☐ No ☐ Yes			
H. Author/Requestor <u>Susan L. Roggenkamp</u> (Print and Sign)		Responsible Manager <u>Vic S. Forney</u> (Print and Sign)	
I. Reviewers		Signature	
General Counsel	Yes ☐	Print _____	Signature _____ Public Y/N (If N, complete J) Y / N
Office of External Affairs	Yes ☐	Print _____	Signature _____ Y / N
DOE-RL	Yes ☐	Print _____	Signature _____ Y / N
Other - <u>LMS I</u>	Yes ☒	Print <u>C. Willingham</u>	Signature <u>Christine Willingham</u> ☒ Y ☐ N
Other	Yes ☐	Print _____	Signature _____ Y / N
J. If Information Includes Sensitive Information and is not to be released to the Public indicate category below. ☐ Applied Technology ☐ Protected CRADA ☐ Personal/Private ☐ Export Controlled ☐ Proprietary ☐ Procurement-Sensitive ☐ Business-Sensitive ☐ Patentable ☐ Predecisional ☐ Other (Specify) _____ ☐ UCNI			
K. If Additional Comments, Please Attach Separate Sheet		Information Clearance Approval

Hanford Year 2000 Business Continuity Plan, November, 1999

S.L. Roggenkamp
Fluor Daniel Hanford Company

Date Published
November 1999

Prepared for the U.S. Department of Energy
Office of Economic Impact and Diversity

FLUOR DANIEL HANFORD, INC.

P.O. Box 1000
Richland, Washington

LEGAL DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

This report has been reproduced from the best available copy.

Printed in the United States of America

Hanford Year 2000 Business Continuity Plan

November, 1999

Approved by:

S.V. Forney, Y2K Project Manager

12/6/99
Date

RELEASE AUTHORIZATION

**Document
Number:**

HNF-5392, Rev. 1

**Document
Title:**

Hanford Year 2000 Business Continuity Plan,
November, 1999

This document, reviewed in accordance with DOE Order 241.1, "Scientific and Technical Information Management," and DOE G 241.1-1, "Guide to the Management of Scientific and Technical Information," does not contain classified or sensitive unclassified information and is:

APPROVED FOR PUBLIC RELEASE

C. Willingham

12/13/99

Lockheed Martin Services, Inc.
Document Control/Information Clearance

Reviewed for Applied Technology, Business Sensitive, Classified, Copyrighted, Export Controlled, Patent, Personal/Private, Proprietary, Protected CRADA, Trademark, Unclassified Controlled Nuclear Information.

LEGAL DISCLAIMER. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, not any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. This report has been reproduced from the best available copy. Printed in the United States of America.

Table of Contents

1.0 OVERVIEW	3
1.1 PURPOSE.....	3
1.2 BACKGROUND	3
1.3 ROLES AND RESPONSIBILITIES	4
2.0 HANFORD'S BUSINESS CONTINUITY PLANNING PROCESS.....	4
2.1 INPUT	5
2.2 KEY ACTIVITIES	5
2.3 THE BUSINESS CONTINUITY DELIVERABLE	7
2.4 Hanford's Y2k Event Description	8
2.5 HANFORD'S BUSINESS CONTINUITY STRATEGY	11
2.6 HANFORDS Y2K EVENT ASSUMPTIONS	13
2.7 HANFORDS CORE BUSINESS PROCESSES.....	15
2.8 BUSINESS IMPACTS/MITIGATION APPROACHES	16
3.0 DRILLS.....	18
4.0 SCHEDULES/MILESTONES AND COST ESTIMATES	20
4.1 SCHEDULE/MILESTONES	20
4.2 COST ESTIMATE.....	21
5.0 SUMMARY OF ZERO DAY PLANS	22
5.1 SCHEDULE OF ACTIVITY	22
5.2 PERSONNEL ON CALL OR ON DUTY.....	22
5.3 CONTRACTOR AVAILABILITY	23
5.4 COMMUNICATIONS INTEGRITY	23
5.5 PROCEDURE SUPPORT	23
5.6 SECURITY CONSIDERATIONS	23
5.7 COMMUNICATIONS WITH THE PUBLIC	24
ATTACHMENT 1: TERMS AND DEFINITIONS	25
ATTACHMENT 2: Y2K CONTINGENCY PLAN GUIDELINES	27
ATTACHMENT 3: ASSURANCE OF MISSION-CRITICAL SYSTEM CONTINGENCY PLAN COMPLETION.....	30

1.0 OVERVIEW

1.1 PURPOSE

The goal of Department of Energy Richland Operations (DOE-RL) Year 2000 (Y2K) effort is to ensure that the Hanford site successfully continues its mission as we approach and enter the 21st century. The Y2K Business Continuity Planning process provides a structured approach to identify Y2K risks to the site and to mitigate these risks through Y2K Contingency Planning, "Zero-Day" Transition Planning and Emergency Preparedness.

This document defines the responsibilities, processes and plans supporting Hanford's Y2K Business Continuity. It further identifies the business continuity drills, schedule and the summary Zero Day Plans that will prepare to monitor and manage Y2k Business Status over the Year 2000 critical period of December 28, 1999 through March 15, 2000; specifically the Rollover Period of December 31, 1999 through January 3, 2000.

1.2 BACKGROUND

Few topics are creating as much interest, or are as widely misunderstood as the approaching Y2K date change problem. There are a number of myths, fallacies and irresponsible assertions circulating about the impact of Y2K failures. DOE-RL's objective is to assess and respond appropriately to the possibility of Y2K failures of both internal systems and external services. In this regard, it is recognized that the Y2K event is different from other natural and manmade events that DOE-RL has addressed. This difference is best described in terms of complexity, humanity and simultaneity.

Complexity - The Y2K date change problem exists in technologically complex systems that influence Hanford operations. Y2K events could emulate from a multitude of sources including internal computers, embedded systems and infrastructure equipment and external services including electrical power and telephones, etc.

Humanity - Y2K is not just a technology issue; people are involved. As such, it is expected that human errors will occur in fixing Y2K problems, addressing foreseen Y2K events or responding to unforeseen Y2K events. The spectrum of human response and choices will occur and their reaction to real or anticipated Y2K events can make things worse.

Simultaneity - Y2K may not be a single event. Y2K failures could be multiple events with varying degrees of severity and duration. In addition, Y2K events could occur before and after January 1, 2000, and a single event could result in a chain reaction.

The Hanford Y2K Business Continuity Planning process is intended to assist the site in reducing Y2K risks by identifying measures to safeguard the ability of the Hanford site to maintain site operations if Y2K events should occur. While it does not offer a long-term solution to Y2K failures, it will help the site prepare for potential Y2K events and facilitate the restoration of normal operations at the earliest possible time and in the most cost-effective manner.

Hanford Year 2000 Business Continuity Plan

The management and technical benefits of Business Continuity planning include:

- Provides DOE-RL management with a high-level overview of the Y2K business risks and solutions
- Ensures DOE-RL management ownership of business operations
- Ensures that Y2K efforts and resources are integrated into existing contingency, disaster recovery and emergency preparedness efforts
- Reduces the potential impact of Y2K events on site operations

1.3 ROLES AND RESPONSIBILITIES

Table 1: Roles and Responsibilities

DOE-RL MANAGEMENT	DOE-RL Y2K COORDINATOR	DOE-RL AMs	CONTRACTORS
Provide Leadership	Develop business continuity guidelines and schedules	Understand risks	Identify internal events
Understand Y2K risks	Identify external events	Identify emergency safe site operations	Identify business impacts
Concur on plans	Prepare Business Continuity Plan	Concur on plans	Prepare/Tests Contingency Plan
Participate in drills, EOC	Ensure IV & V is performed	Provide direction to contractors	Prepare Y2K Emergency Management Plan
Provide resources	Monitor, track & report status	Fund activities	Form IT and facilities SWAT Teams
	Share and prepare corrective actions		Implement plans
Communicate	Communicate	Communicate	Communicate

2.0 HANFORD'S BUSINESS CONTINUITY PLANNING PROCESS

The Hanford BCP Process can be described in four general phases:

- (1) Planning - Identifying Y2K events that could have a negative consequence on the site's business and operations, and defining a set of appropriate management actions. (2) Prevention - Assessing risks to the site, and taking actions that reduce the probability of a Y2K event occurrence (event mitigation).

Hanford Year 2000 Business Continuity Plan

(3) Preparation - Preparing for the possibility that the Y2K event will occur and creating necessary contingencies. This includes establishing procedures, and conducting tests and drills.

(4) Performance – Preparing Y2K contingency and emergency preparedness plans. Executing zero day plans to monitor core businesses, systems and projects.

2.1 INPUT

The input to this approach includes both the GAO Y2K business continuity and contingency planning guidelines, GAO/AIMD – 10.1.19 and the DOE-HQ Directives and Guidance dated January 28, 1999.

2.2 KEY ACTIVITIES

2.2.1 Y2K Business Continuity Planning

The risk of Y2K failures is not limited to internal computer systems but include potential failure of embedded microprocessors installed in buildings and process control systems. Hanford also depends on information and data from our business partners – including other federal agencies, state and local agencies. Finally, Hanford relies on external electrical power telecommunications and local security services. Y2K failure of our business partner or external service provider is also a risk that must be addressed.

Figure 1: Hanford Business Continuity Planning Process

The key elements of Hanford's Y2K Business Continuity Planning are (1) establish the Y2K event and site wide strategy (2) identify core business processes (3) perform Y2K impact/mitigation analysis (4) identify emergency safe operations (5) obtain field managers concurrence of draft BCP and CPs (6) conduct tests and drills and (7) finalize BCP, CPs and EPP

DOE-RL, with support of the site contractors, will identify those systems and services that are required to maintain emergency-safe operation. Emergency-safe operations are those services and systems required by the site to protect the health of onsite and offsite personnel, to protect the environment and to provide adequate security.

2.2.2 Y2K Contingency Planning

The objective of contingency planning is to reduce potential impacts of Y2K events for systems and services necessary for emergency safe operations. DOE-RL will prepare contingency plans for each core business process and develop procedures for alternative solutions and/or compensatory actions to reduce the impact of Y2K events to acceptable levels. Contingency Plans may be produced for specific systems and/or facilities or projects. They may or may not include "Zero-Day" Transition Plans. It is not necessary to develop a separate contingency plan for each system/service identified as it may be appropriate to develop a single plan for a facility or a system that covers several operating locations.

Contingency plans will be tested to ensure that procedures can be implemented successfully if a Y2K event occurs and train the appropriate personnel to ensure personnel efficiency in the event the plans are activated. It is recommended that Y2K events and procedures that activate the Y2K Contingency Plan and events, and procedures that terminate Y2K Contingency Plans be considered.

2.2.3 Execute Plans

Contingency plan execution consists of the actions taken prior to a potential Y2K event (preemptive) and after the occurrence of a Y2K event (either post incident or reactive response). It includes monitoring of contingency triggers and implementation of contingency operations.

Preemptive Measures - Activities implemented prior to the occurrence of a Y2K event, i.e. verifying the Y2K readiness of essential service providers contracting for alternate services; stockpiling of critical supplies; staffing the Emergency Operation Center; shutting down systems and facilities and staging personnel on-site prior to the millennium change.

Post-Incident Actions - Activities implemented after the event, i.e. monitor events as it moves around the world; phased startup of facilities and equipment; implementation of manual operations and communications with major service providers.

Reactive Measures - Activities implemented when a Y2K event occurs i.e. activate business response teams to minimize spread and duration of problem; activate contingency and disaster recovery plans. Activate facility response team.

2.2.4 Continue Operation

This activity includes restoring/restarting systems and services as required and the notification of appropriate authorities of operational status or problem resolution.

2.2.5 Communications - Zero Day Reporting

DOE-RL and the site contractors will monitor, track and report progress for the Y2K business continuity planning efforts. In addition, DOE-RL will institute an awareness and communications program including presentations, briefings, seminars and publications to ensure site personnel and local residents are fully aware of DOE's Y2K activities and contingency planning. Finally, Communications to the public through press releases will be planned as part of the Zero Day Activities from December 28, 1999 through January 3, 2000.

2.3 THE BUSINESS CONTINUITY DELIVERABLE

The key output of this planning effort is illustrated in Figure 1.

Figure 2: Y2K Business Continuity

Y2K Contingency Plans - An operational plan, which describes the steps a system owner plans to take to ensure that the functionality of a system is maintained in the event of an internal or external Y2K-related failure. Attachment 2 contains the Contingency Plan Guidelines. This plan should not be confused with the DOE-HQ requirement to prepare a contingency plan for a system that fails to meet the validation milestone date of February 15, 1999. The specific contingency plans generated from this effort will be kept as a working document in the Y2K Project Office for the life of the Zero Day Plans and then they will be managed as a record according to Hanford Document Control Process/Procedures.

Y2K Emergency Preparedness - Identifies the specific emergency response actions and procedures for a Y2K event(s). (It utilizes the Emergency Preparedness Plans and infrastructure currently in effect at Hanford).

Zero-Day Transition Plan - Identifies specific zero-day transition actions and procedures for the period between December 30, 1999 and January 4, 2000, and February 28, 2000, through March 1, 2000. It identifies roles and responsibilities, schedules security and communications with the public.

2.4 Hanford's Y2k Event Description

Based on information from several sources, such as Bonneville Power Administration (BPA), Washington State and other industries, the Hanford Y2K event falls into two categories, external and internal. External events are defined as the possible failure of offsite systems which, in some manner, interface or provide services or products to the Hanford Site. Examples of an external event include loss of electrical power, disruption of phone service, and loss of transportation. Internal events are defined as the possible failure of onsite systems, such as software applications, equipment items, or onsite telecommunications.

Following is a graph that identifies the probabilities and the approximate times when Y2K events are most likely to occur on the Hanford Site:

Figure 3: Y2K Risk Levels

2.4.1 Electrical Power

Delivery of electrical power to the Hanford Site is divided into three segments: generation, transmission and distribution. Each of these segments is owned and operated by different entities and each may have a different Y2K-related risk.

Electric power generation for the Hanford Site is a combination of hydroelectric, thermo (coal, gas, etc.) and nuclear. This diversity of power generation is viewed as an advantage. The chance of having a simultaneous failure that would affect all generators is considered to be low. The Site is also fortunate that it has a 100-megawatt nuclear power plant feed connection at the same substation from which the Site acquires its power.

The transmission system that delivers electrical power to the Hanford Site is owned and operated by the BPA, and has been in existence since 1937. The Y2K risk to the transmission system is much less than the Y2K risk to the generation segment. The transmission system is comprised of wires and poles. The greatest Y2K risk involves the communication system that is used to

control devices such as circuit breakers and switches. The use of voice communication and the staging of additional personnel in key locations, such as substations, could mitigate this risk.

The electric power distribution system on the Hanford Site is a combination of Hanford Site and BPA-owned and operated systems. The Y2K risk associated with the distribution system is similar to that of the transmission system. It is made up of basically the same components that comprise the transmission system. The onsite utility group works directly with BPA on a regular basis, and will continue to do so to ensure that communications are maintained during the Y2K rollover.

Another issue, which is associated with the reliability of the electrical power, involves the impact that the consumer may have on the power system. During a period starting on January 1, 2000, there is a possibility of intermittent power failures due to a major consumer of power dropping off the power system because of Year 2000 failures in their operations. This loss of a major electrical load could cause instabilities in the power grid, causing one or more of the power system components to shutdown.

The Y2K impact to the Hanford Site could be an intermittent/continuous disruption starting on January 1, 2000, and extending over a period of 60 days. Planning for this event should assume a 3-day minimum disruption both for operations that impact personnel health, safety, security and environmental impacts.

2.4.2 Telecommunications

Telecommunications is a key system on the Hanford Site functions, and the loss of these systems would cause a major disruption. The telecommunication system utilized is a combination of on-site and off-site components. The site, as it is configured, provides telephone service through a site-owned and operated telephone switch located in the 300 Area. This switch provides phone service to the majority of the site facilities, including leased facilities and the Federal Building. The phone switch also provides the ability to communicate off-site.

The components that make up the on-site and off-site telecommunication system are very similar in nature. The systems are mainly electronic switches and cables. The main component that is at risk involves the billing systems. Although the failure of the billing system would be an inconvenience, the main function of the switch would not be affected. Consequently, very few system reliability problems are expected to occur. However, on January 1, 2000, there may be an unprecedented volume of calling (e.g., many times that of

Mother's Day). The main problem may be a "busy signal," rather than any date-related problem. Because the high off-site call volume should not affect the on-site phone system, the internal telecommunication system should be at a low risk of failure.

The Hanford Site could be impacted by high call volume for a period of two days starting January 1, 2000 for offsite telecommunications.

2.4.3 Transportation

Transportation involves the ability to obtain supplies and services to support daily operations. With the advent of "Just-In-Time" warehousing, many suppliers keep a limited supply of goods on hand. The ability to replenish goods quickly depends on all types of transportation. Supplies that could be affected may include delivery of food, fuel, and repair parts. As with supplies, a number of services may be affected by a disruption in transportation, such as emergency services. The risk associated with transportation is not easily defined.

Transportation is made up of several systems ranging from the computerized dispatching systems, to the physical vehicles, such as trucks and airplanes, all of which could be affected by a Y2K issue. For the Hanford Site, this impact could be a delay in services during the period January 1, 2000 to January 7, 2000.

2.4.4 Security

In recent years, local protection agencies have been enlisted to augment the Hanford Patrol. During the transition to the Year 2000, the Hanford Site may experience an increased risk of a security breach. Because of the time of year (winter and New Years Eve) the local protection agency may not be able to respond as quickly, or in large enough numbers, to avert a security event.

The Y2K event could impact the site's ability to maintain security and other law enforcement activities for a period from January 1, 2000, to January 3, 2000.

2.4.5 Internal Systems

194 PHMC Y2K projects were implemented and validated by July 31, 1999. Based on industry analysis, there is an expected five percent failure rate of the systems that have been renovated for Y2K. These failures may be due to injecting new errors while renovating program code for Y2K and for issues that were not identified during assessment. This equates to a possible Y2K failure of ten systems on the Hanford Site.

Table 2 summarizes the Hanford Y2K events description.

Table 2: Y2K Event Description Summary

SERVICE/ SYSTEMS	PROBABILITY OF OCCURRENCE	FAILURE PERIOD	Y2K EVENT DESCRIPTION
Telecommunication	High	12-30-99 to 1-2-00	<ul style="list-style-type: none"> Intermittent interruptions over 2 day period
Security	Moderate	12-30-99 to 1-3-00	<ul style="list-style-type: none"> Attempted breach of security over 3 day period

Table 2: Y2K Event Description Summary Continued

SERVICES/ SYSTEMS	PROBABILITY OF OCCURRENCE	FAILURE PERIOD	Y2K EVENT DESCRIPTION
Electrical Power	Moderate	12-30-99 to 3-1-00	<ul style="list-style-type: none"> Intermittent disruptions of up to 3 days over a 60 day period
Transportation	Moderate	12-30-99 to 3-1-00	<ul style="list-style-type: none"> Delays of 1-2 days over 14 day period
Internal System	High	1-2-00 to 0-4-00	<ul style="list-style-type: none"> 5% of internal systems will experience Y2K failures

2.5 HANFORD'S BUSINESS CONTINUITY STRATEGY

Hanford's Y2K Business Continuity planning strategy is illustrated in Figure 4, and is summarized as follows:

- Prior to December 31, 1999, the Site will initiate cost-effective, preemptive actions that will reduce the potential impact of Y2K events on site-operations.
- On December 29 and 30, 1999, the site will initiate a time-phased curtailment of site operations consistent with normal weekend operations and designated preemptive actions.
- On December 31, 1999, the site will initiate either a time-phased curtailment or startup of site operations based upon real-time assessment of both external and internal Y2K events.

Figure: 4 Hanford Business Continuity Strategy

The actions that may be implemented are illustrated in Figure 4. This figure identifies December 31, 1999 as the baseline for determining if an action is defined as Preemptive, or Post Incident.

2.5.1 Preemptive Actions

Preemptive actions are steps to be taken prior to December 31, 1999 to minimize or mitigate Year 2000 impacts. The proper identification of preemptive activity will greatly reduce the need for post-incident actions. The following is a list of the major preemptive actions that will be implemented.

- Staff the Emergency Operations Center prior to the year 2000 transitions.
- Stage additional personnel at critical facilities.
- Reduce the operational levels of non-critical facilities.
- Stockpile critical supplies (generators, batteries, fuel etc.).

2.5.2 Post Incident Actions

Post Incident Actions are those actions that will be implemented based on identified triggers. Triggers are defined as events or predefined points of time when an action will be implemented. Examples of triggers could include the loss of electrical power or the failure of an automated system. Just as with the preemptive actions post incident actions may be implemented at a site-wide or at a facility level. The following is a list of Post Incident Actions that may be implemented to assure the safe operations of the site:

- The shutdown of a facility or system.
- The Implementation of a predefined contingency plan
- Operate utilizing a manual procedure
- Mobilize additional personnel
- Implement alternate means of communication
- Utilize backup power

- Activation of a Year 2000 "SWAT" team to repair a failed system.

The above lists identify actions that could be implemented due to events or failures. The specific facility actions will vary based on operational needs and the level of support that it must provide to the site. Site wide actions required should fall mainly into the preemptive category. As stated above, the preemptive active can greatly reduce the number of post incident actions that may need to be implemented. The BC strategy is a critical part of preparing for the Year 2000 transition.

2.6 HANFORDS Y2K EVENT ASSUMPTIONS

The following defines the Hanford Y2K event assumptions that describe the site wide services to be available/unavailable.

TABLE 3: Available Systems/Services

Y2K EVENT ASSUMPTIONS	
•	Site-wide telephone, two-way radio, and telephone "85-paging" systems will be available.
•	Fire notification systems (RAFAR) will be operational for 48 hours after the loss of electrical power.
•	Emergency response personnel will be available (fire, patrol).
•	Site emergency alarm systems will be operational (cash phones, siren).
•	Site water system and sanitary sewer system will be operational (K Basin will have potable water only- <u>NO</u> firewater, 100N will have firewater only- <u>NO</u> potable water).
•	Natural gas to the site will be available.
•	Emergency operations center (EOC) will be staffed from December 31, 1999 until event completion and will provide site-wide Y2K coordination and communication
•	If an electrical power outage occurs, electrical power will be restored on priority basis.
•	Diesel fuel can be stored in 200W area if required
•	Gasoline will be available throughout the event at 200E and 100 area stations.
•	Any modifications to the fire protection/suppression systems (i.e.: draining of pipes, etc.) will be performed by the Hanford Fire Maintenance Department.
•	Essential personnel will be assigned to shifts over the time period of concern.
•	Assigned personnel are responsible for getting to and from work on their assigned shifts and providing they're own food.

Table 5: Unavailable Systems/Services

Y2K EVENT ASSUMPTIONS	
•	Dosimeter readings will not be made during the period January 1, 2000 through January 7, 2000.
•	Whole body counter will not be available during the time period of January 1, 2000 through January 7, 2000.
•	The PHMC central computing facility (BLDG 339A) will not be available from December 30, 1999 until reliable, stable electrical power is available (no sooner than

Hanford Year 2000 Business Continuity Plan

January 2, 2000).

- JCI package boilers will NOT be available unless they have auxiliary power.

Hanford Year 2000 Business Continuity Plan

2.7 HANFORDS CORE BUSINESS PROCESSES

Table 6: Core Business Processes

COMPANY	BUSINESS AREA	CORE BUSINESS PROCESS
PHMC	PROJECTS AND FACILITIES	<ul style="list-style-type: none"> • BWHC-300 Area • BWHC-FFTF • BWHC-PFP • BWHC-WESF/FASTER • DESH-SNF • LMHC-TWRS • WMH-Solid Waste Operations • WMH-Liquid Effluent Operations • WMH-Analytical Laboratory Operations • WMH-Data Systems
	SITE COMMUNICATIONS	<ul style="list-style-type: none"> • FDH Telephone System • FDH Two-way Radio • FDH Site-paging • FDH Hanford Local Area Network (HLAN)
	SAFETY & SECURITY	<ul style="list-style-type: none"> • FDH Nuclear Safety • FDH Environmental Protection • FDH Radiation Protection • FDH Occupational Safety • FDH Fire Protection • FDH Security Protection • FDH Hanford Emergency Management
	SITE UTILITIES AND SERVICES	<ul style="list-style-type: none"> • DYN Electrical Utilities • DYN Water Utilities • DYN Sewer Utilities • DYN Transportation Operations • DYN Fleet maintenance • DYN Materials Management
	BUSINESS MANAGEMENT	<ul style="list-style-type: none"> • FDH Financial Management • FDH Production Services
PNNL	PNNL	<ul style="list-style-type: none"> • Facilities & Operations • Financial Processing System • Hanford Environmental Dosimetry Program • Human Resources Information System
BHI	BHI	<ul style="list-style-type: none"> • Business Application • Ground Water
HEHF	HEHF	<ul style="list-style-type: none"> • Medical Surveillance Program

2.8 BUSINESS IMPACTS/MITIGATION APPROACHES

Table 7: Business Impact/Mitigation Approach

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• BWHC-300 Area	• Potential frozen pipes & facilities damage	• Implement pipe draining process
• BWHC-FFTF	• Loss of plant HVAC/lights	• Operate @ "Minimum-Safe" condition (existing contingency plans)
• BWHC-PFP	• Loss of plant HVAC/control system	• Operate @ Minimum-Safe" condition (existing contingency plans)
• BWHC-WESF/FASTER	• Loss of plant HVAC	• Operate @ "Minimum-Safe" condition (existing contingency plans)
• DESH-SNF	• Shutdown of facility and construction operations	• Operate @ "Minimum-Safe" condition (existing contingency plans) implement manual operations
• LMHC-TWRS	• Undefined until study complete	• TBD
• WMH-Solid Waste Operations	• Facility Shutdown	• Implement existing facility & systems Contingency plans
• WMH-Liquid Effluent Operations	• Shut down of operations	• Shut down operations • Implement existing shutdown procedures
• WHM-Analytical Laboratory operations	• Facility shutdown • Corrupt database	• Operate " @ "Minimum-Safe" condition • Shutdown data base
• WMH-Data Systems	• Inability to provide reports	• Prepare reports manually/delay reporting

Table 8: Safety and Security

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• FDH-Environmental Protection	• Inability to provide reports	• Perform manual operations
• FDH-Radiation Protection	• Inability to establish access eligibility	• Provide qualification records prior to event
• FDH-Occupational Safety	• Inability to provide OSHA reports	• Manually prepare forms
• FDH-Nuclear Safety	• Inability to provide reports	• Perform manual report preparation

Table 9: Site Communication

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• FDH-Telephone System	• Loss of telephone service after hours	• Install portable generators/ provide technical support
• FDH-Two-way Radio	• Degradation of communications after 12 hours.	• Install portable generators at selected sites
• FDH-Site Paging	• Loss of paging service after hours.	• Upgrade telephone system
• FDH-Hanford Local Area Network (HLAN)	• Loss of service/damage to equipment	• Install electrical surge protection devices

Table 10: Site Utilities and Services

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• DYN-Electrical Utilities	• Loss of substation power	• Install portable generators, heaters & two-way radios
• DYN-Water Utilities	• Extended operation of backup electrical generators • Potential pipe freezing	• Ensure adequate manpower to support operations • Implement freeze protection plan
• DYN-Sanitary Services	• Extended operation of sewer lift stations	• Ensure adequate manpower to support operations
• DYN-Transportation Operations	• Inability to start vehicles (cold temp)	• Install portable generators
• DYN-Fleet Maintenance	• Inability to provide vehicle fuel • Inability to provide maintenance support	• Install portable generators
• DYN-Materials Management	• Unable to provide logistic support	• Curtail operations to essential personnel only
• FDH-Production Services	• Damage to computer equipment • Facility damage (cold weather)	• Curtail operations during high risk periods • Drain pipes if necessary (cold temp)

Table 11: Business Management

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• FDH-Financial Management	• Delay of payroll and accounts payable	• Perform manual operations

Table 12: PNNL

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• Facilities & Operations	• TBD	• TBD
• Financial & processing System	• System unavailability • Inability to send or receive files	• Manually create entries
• Hanford Environmental Dosimetry Program	• Loss of business function	• Perform manual calculations • Utilize backup services
• Human Resources Information System	• System unavailable	• Early preparation of payroll checks

Table 13: BHI

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• Business Application	• Disruption of operations	• Pre-execute financial transactions
• Ground Water	• Freezing of pump hose pipes	• Install heaters

Table 14: HEHF

CORE BUSINESS PROCESS	EVENT IMPACT	MITIGATION
• Medical Surveillance	• Inability to perform business functions	• Curtail operations to essential personnel only

3.0 DRILLS

The following table identifies the Y2K drills to be performed.

Table 15: Y2K Business Continuity Drills

DATE	OBJECTIVE
4-9-99	• Validate alternative communication process and train personnel
9-9-99	• Validate PHMC Y2K readiness through simulations of loss of electricity and Y2K date failures (tabletop exercises of select systems).
11-18-99	• Validate PHMC's EOC readiness through simulation of Y2K event.

April 9, 1999 Drill

The purpose of this exercise was to train and familiarize onsite and offsite electrical utility personnel with alternate communication processes. The Site Emergency Response Organization participated by exercising communication links with department of Energy Headquarters

Emergency Operation Center (EOC). The exercise validated actions to be taken for events associated with Y2K related infrastructure and supporting system failures. In addition, this drill served as the basis for identifying modifications required in current strategies and contingency planning for Y2K related events.. The scenario was based upon credible events identified during Y2K readiness assessments. The scope of the exercise participation was limited to the EOC, Bonneville Power Administration (BPA) and site electrical utility personnel.

During the observation of the exercise the following opportunities for improvement were identified:

The need to extend the range of the VHF radio provided to BPA

Provide written formal procedure on the operation of the VHF radio provided to BPA

September 9, 1999 Drill

The purpose of this tabletop drill was to train and familiarize participants with the monitoring and progress reporting process and associated responsibilities that will be used during the rollover to the year 2000 at the Hanford Site. Drill participants included the Site Emergency Response Organization, DOE-RL, and key individuals from each of the Site major contractors. The drill was arranged as a tabletop to provide an opportunity for key process individuals to meet collectively, become familiar with their roles and responsibilities discuss and discern the process and provide feedback for revisions and enhancements. In addition, the drill served as a basis for identifying modifications required to the reporting process, current strategies and contingency planning for Y2K related events. The tabletop drill involved two scenarios. The first scenario assumed that no problems, Y2K related or otherwise, were encountered. The second scenario introduced weather and system problems.

During the Observation of the exercise the following opportunities for improvement were identified:

Investigate the common failure points of the selected zero-day communication methods and determine whether the prioritization method is still appropriate.

Develop a separate process for monitoring and reporting classified system status.

Determine information security considerations that should be incorporated into the monitoring and reporting process.

Require all rollover points of contact to carry an 85-pager. Incorporate those pager numbers into the contact list.

Develop a Y2K tip sheet for those involved in the zero-day process that includes considerations and reminders as year 2000 approaches (e.g., charged/fresh pager batteries, ISDN phones will not work if power is out – only 'standard' handsets will work), publish list of essential IT personnel and backups, etc.)

- Prepare several General Delivery messages during December with items that the general Hanford populace should be aware of (e.g., overview of rollover process, turn off PCs, reduce power consumption, etc.)
- Determine the work schedule for the Y2K Event Coordination Team during the rollover timeframe.

- Develop what criteria will terminate the Y2K Event Coordination Team prior to January 3, 1999.
- Ascertain what alternate communications and prioritization processes DOE HQ is using.
- Determine senior management expectations for reporting Y2K status.
- Determine the need for clearances to handle classified system status for those that will be at the Hanford Emergency Operations Center during the rollover.

November 18, 1999 Drill

The purpose of this drill was to exercise the Emergency Operations Center Staff and Y2K Participants. For this drill, a scenario was prepared to simulate a December 31, 1999 cold weather blast hitting the site along with Y2K rollover. The weather driven event was planned to simulate numerous site related infrastructure failures causing the EOC to make decisions based on the cumulative effect of the degrading conditions.

4.0 SCHEDULES/MILESTONES AND COST ESTIMATES

4.1 SCHEDULE/MILESTONES

Table 16: Schedule/Milestones

BUSINESS CONTINUITY MILESTONES	
• DOE-HQ Business Continuity Directive.....	01/28/99
• Conduct Y2K awareness exercise.....	04/09/99
• Issue draft BCP and CP's.....	04/30/99
• Complete CP tests.....	08/01/99
• Issue Final BCP and CP's.....	08/30/99
• Complete Drills.....	11/30/99

Hanford Year 2000 Business Continuity Plan

4.2 COST ESTIMATE

The estimate cost to support the business continuity effort is \$490,000 and \$338,000 for FY 1999 and FY 2000. The major cost drivers are three fold:

1. Upgrade Telephone, Two-Way Radio and "85-Pager system" - this activity includes the procurement and installation of backup electrical power generators. (\$285K)
2. Upgrade TWRS Facility - this activity includes the engineering, procurement and installation of backup electrical generators for two TWRS facilities. (\$150K)
3. Modify TWRS Procedure - this activity is intended to identify and modify TWRS operating procedures to accommodate the Y2K planning event (\$160K)

Table 17: Cost Estimate

COMPANY	MSC COMPANY	FY 1999 COST	FY 2000 COST	TOTAL
PHMC	BWHC	10K	10K	20K
	WMH	20K	10K	30K
	LMH	270K	130K	400K
	DYN	-	65K	65K
	DESH	5K	25K	30K
	FDH	185K	98K	285K
PNNL	TBD	TBD	TBD	TBD
BHI	TBD	TBD	TBD	TBD
TOTAL		490K	338K	830K

5.0 SUMMARY OF ZERO DAY PLANS

The Y2K Zero Day Plan at Hanford begins on December 28, 1999, continues until March 15, 2000, consists of two different status reporting timeframes, includes a contractor status validation, and provides communication to Site senior management, employees and the public. The period of intense Y2K awareness and concern at the Hanford Site is the period immediately on either side of the date transition from December 31, 1999 through January 2, 2000 and is called Y2K Rollover Period.

5.1 SCHEDULE OF ACTIVITY

The Hanford Site will be in a minimum safe mode prior and during the rollover period due to holidays and Y2K planning. During this timeframe, key site individuals will be positioned to monitor status of active Y2K projects. A Y2K Event Coordination Team will be stationed at the Hanford Emergency Operations Center to collect and evaluate project information, submit reports to DOE-HQ and provide status to senior management and the public. This team will remain active until the morning of January 3, 2000 or until such time that Site operations are determined to be stable. If the team disbands prior to January 3, the normal Site emergency and occurrence notification processes will be used should any problems arise. From a Site perspective, rollover to the year 2000 will be managed similarly to other potential Hanford events because of the significance and potential risks of date-related issues. Although Y2K monitoring and reporting will take place, this status reporting does not alter any existing requirements and procedures for reporting occurrences and emergencies (per DOE O 232.1A and DOE O 151.1).

Most Hanford systems will not be active until January 3, 2000 when Site operations go back to normal after the holiday. As such, monitoring and tracking will continue but the process will be slightly different than over the weekend. Beginning the morning of January 3, 2000 each contractor will continue to collect Y2K status information and instead of reporting to the Y2K Event Coordination Team, will report directly to the DOE-RL Y2K Project Manager. This information will then be used to submit reports to DOE-HQ. Status reporting will continue in this manner until March 15, 2000 at which time all Y2K projects and systems should have reported their Y2K status and any problems should have been resolved. Each Hanford contractor will be requested to submit a Y2K validation letter to finalize status reporting.

5.2 PERSONNEL ON CALL OR ON DUTY

Essential personnel have been identified within each of the site contractor organizations and within DOE-RL through the execution of this Plan. Site Emergency Preparedness (EP) organizations will use existing on-duty/on-call procedures. Personnel are being familiarized (through drill participation) with expectations for the rollover, including communications and reporting procedures for Y2K systems. Computer technicians, facility managers, procurement specialists, external affairs representatives, EP personnel, site Y2K project representatives,

and site senior management representatives have all been identified for duty or on-call availability.

The Hanford Y2K Project office continues to maintain the Business Continuity Plans, a summary BCP event trigger list and the schedule of active systems. The aforementioned documentation shows when all systems plan to be active on or after the rollover and provides primary and secondary points of contact information for Hanford Y2K Mission Critical, Essential and Safety Systems.

5.3 CONTRACTOR AVAILABILITY

Each of the sites' Prime Contractors has committed to being available during the Y2K rollover. In addition, site vendors who provide fuel services (CONOCO), power (BPA), telecommunications (US West), well as external (county) patrol services are also committed to being available during the Y2K rollover.

5.4 COMMUNICATIONS INTEGRITY

DOE-RL will rely on a number of redundant communications paths. Backup power generators have been leased and will be installed at site telecommunications hubs to ensure continued operation of site pagers and radios. The previously established EP infrastructure allows us the ability to communicate with local public agencies through the use of site radios. Assuming the external telephone network remains operational, DOE-RL will obtain a Government Emergency Telephone System (GETS) card, which will allow priority calling in the event of heavy telephone traffic. Communications Processes and Redundancy Have been the subject of Y2K Drills on April 9, 1999 and November 18, 1999.

5.5 PROCEDURE SUPPORT

Previously established EP procedures (e.g., winter storm – site closure procedures) will be invoked as necessary. These procedures and processes have been exercised in the September 9, 1999 Y2K Tabletop Drill, the October 8, 1999 Cold Weather Drill and the site limited exercise of November 18, 1999.

5.6 SECURITY CONSIDERATIONS

Access to the Internet will be adjusted prior to rollover to restrict access of the Hanford Local Area Network (HLAN) from the Internet. Communications from HLAN to the Internet will be open, however E-mail access to HLAN from the Internet will be "turned off" during the rollover period of December 28, 1999 through January 2, 2000. Full Access to the Internet from HLAN will resume after review of firewall activity and the Internet by Internet security personnel at Hanford. A security contact will be on hand as part of the Y2K Event Coordination Team for the rollover period. This is a normal part of existing procedures for reporting occurrences and emergencies. Contacts have been made with the local sheriff's department, the DOE Inspector General's (IG) office and the FBI, in the event that support from these organizations are required during the rollover or thereafter.

In addition, The Y2K Project Office will conduct a security review of the BCP, contingency plans, procedures and Y2K Files. The reviews will ensure the safety of Hanford information through the heightened activity prior and during the rollover period and address and avoid any "mosaic effect" issues.

5.7 COMMUNICATIONS WITH THE PUBLIC

The Y2K Event Coordination Team stationed at the Hanford Emergency Operations Center will provide status to site employee's senior management and the public after rollover information has been evaluated. Communications and press releases have been planned as part of the rollover reporting process. The DOE-RL Office of External Affairs will be represented on the Event Coordination Team to facilitate external communications as required.

ATTACHMENT 1: TERMS AND DEFINITIONS

Y2K Business & Operations Continuity - The process of maintaining emergency-safe site operations after the occurrence of foreseen or unforeseen Y2K events.

Y2K Business & Operations Continuity Planning - The process of identifying Y2K risks, assessing the impact on site operations and the development and implementation of risk reduction strategies including site-wide project-specific Y2K Contingency Planning, "Zero-Day" Transition Planning and Emergency Response.

Emergency-Safe Site Operations - Those systems and services required by the site to protect the health of onsite and offsite personnel, to protect the environment and to provide adequate security.

"Graded" Business Continuity Approach - Establishes extent of business continuity activities commensurate with identified Y2K risks. That is, a high Y2K risk would result in extensive contingency planning activities; whereas, a low Y2K risk would result in minimum contingency planning activities.

Systems - Y2K mission essential and other than-mission critical systems.

Services - Products and services used to support Y2K mission essential and other than mission essential systems.

Service Provider - Any company, federal or state agency that provides goods or services to the site.

Y2K Event - A Year 2000 induced failure that has an impact on a system or service (i.e., computer shutdown, loss of transmission)

External - From outside site (e.g., from DOE-HQ, from other sites, from other companies/subcontractors)

Internal - From inside site (e.g., people assigned at the site, local DOE, etc.)

Y2K Contingency Planning - The process of identifying alternate solutions and compensatory actions taken to counteract unacceptable foreseen and unforeseen Y2K events. (Includes Disaster Recovery Planning)

"Zero-Day" Transition Planning - The development of site-wide actions and procedures to be implemented on key Year 2000 dates to address foreseen Y2K problems and to respond expeditiously to unforeseen Y2K events. For example, from September 30, 1999 to October 1, 1999, December 30, 1999 through January 1, 2000; and February 28, 2000 through March 1, 2000.

Emergency Preparedness - Identifies the specific emergency response actions and procedures for a Y2K event(s). (It utilizes, as much as practical, the Emergency Preparedness Plans and infrastructure currently in effect at each DOE site.)

Y2K "Readiness" Monitoring and Reporting – The process of monitoring, tracking and reporting progress of the DOE sites in performing Y2K Business Continuity Planning and Implementation activities.

Year 2000 Compliance - Year 2000 Compliance means that a system or application is either *fully compliant or Y2K ready*.

Note: The industry generally refers to this definition as Y2K readiness.

Fully Compliant - Fully compliant means the operation, performance and functionality of a system is not affected by dates prior to, during and after the year 2000. This includes all existing data interfaces/exchanges to or from the system. In particular, the following rules are satisfied:

Rule 1 - General Integrity - No value for current date will cause any - Date-based functionality must behave consistently interruption in operation.

Rule 2 - Date Integrity prior to, during and after the year 2000.

Rule 3 - Century Integrity - In all interfaces and data storage, the century in all dates must be specified either explicitly or by unambiguous algorithms or inference rules.

Rule 4 - Leap Year Integrity - Year 2000 must be recognized as a leap year.

Note: Industry refers to "fully compliant" as simply "compliant".

Y2K Ready - Y2K Ready means that, although a system or application is not fully compliant, it has been determined to be suitable for continued use into the year 2000. Solutions such as rolling back the system clock, use-as-is, retirement, manual work-arounds are examples of being Y2K ready.

ATTACHMENT 2: Y2K CONTINGENCY PLAN GUIDELINES

This document describes a proposed format and content of a Y2K contingency plan. The plan should address the following items.

- Objective
- Plan Duration
- Criteria/Triggers
- Roles, Responsibilities, Authorities
- Plan Testing
- Operating in Contingency Mode
- Resource Plan

OBJECTIVE

The specific objectives of the plan must be clearly identified (e.g., continue in a degraded mode or abort the business function as quickly and as safely possible). If the Y2K contingency plan is for, foreseen Y2K event state the impact, desired work-around or operational level and remaining functionality. Separate any roles, procedures, responsibilities and actions for foreseen versus unforeseen Y2K events.

CRITERIA/TRIGGERS

Identify trigger points or criteria for when the contingency plan will be implemented. The triggers or criteria may equate to a level or event.

PLAN DURATION

Identify the implementation and termination (if applicable) dates of the plan. The expected duration could be as short as a few hours for cases with relatively quick fixes; however, it may be indefinite. Identify what events, activities or results would terminate the plan.

A Y2K contingency plan may be established as a standard operating procedure or it may have a specified life span that is based on the occurrence of certain criteria. The contingency plan will specify how the plan will be maintained throughout the life of the system or terminated.

ROLES, RESPONSIBILITIES AND AUTHORITIES

Define management, technical, operations, and the Year 2000 Project Office personnel roles and responsibilities for executing the provisions of the plan. An organization chart with assigned authority is useful. Identify the process for emergency notification of all impacted personnel, which should include site management and the Year 2000 Project Office.

PLAN TESTING

Identify how the plan will be tested to ensure actual Y2K events can be handled as identified in the contingency mode procedures. The items to be considered for testing include:

- Approach
- Objectives
- Expected outcomes
- Roles and responsibilities
- Testing team, equipment, other resources
- Training requirements
- Schedule
- Test location
- Exit criteria

The testing should validate the functionality of the contingency procedures. Examine results for accuracy and consistency and note discrepancies. Ensure that:

- there is adequate capability to manage, record and track the contingency transactions through the alternate business process
- manual activities (in particular) and the alternative business process (in general) meet an acceptable performance
- an acceptable level of quality control is provided to critical parts of the alternate business process, and an acceptable level of integrity and consistency is provided to alternate databases
- contingency database requirements are defined for alternate implementation modes, and contingency bridges can provide conversion from the contingency environment back to the normal production environment
- any functional differences between the normal business process and the alternative business process can be reconciled or adjusted at the database level.

OPERATING IN CONTINGENCY MODE

Criteria for Invoking a Contingency Mode

Address the criteria that activate the plan (e.g., reaching the Y2K event date, experiencing serious system failures, incorrect dates, etc.). In other words, what events or dates indicate that a contingency mode of operation must be put in place? This criterion is referred to as a trigger and is included in the Y2K project schedule once the contingency plan is approved.

Procedures for Invoking Contingency Mode

Describe the procedures for initiating the Y2K contingency plan. If the plan covers a range of Y2K contingencies, it identifies the procedures used for implementing each of the various conditions (i.e. recovery from loss of data files, loss of a major component of hardware,

transfer to an alternate processing location, etc.)

Procedure for Operating in Contingency Mode

Provide specific operating procedures for all Y2K events and triggers. Consideration should be given the three basic operating modes:

- **Manual** - Required when the system or equipment is completely inoperable and all processes have to be done manually (e.g., manual readings, calculations, file/data transfers, reports, etc.) to maintain minimal functionality.
- **Semi-Automated** - The use of Y2K compliant hardware and software tools and personnel to maintain system functionality.

Criteria for Returning to Normal Operating Mode

Establish the criteria that indicate a system/service can be restored to normal operation. In some instances, the original system will never be used again and the contingency plan should identify the procedures that deactivate or replace the original system.

Procedure for returning to normal operating mode

Describe the procedures to restore or restart the system/service. The procedure should include procedures to correct and restore corrupt/loss data and should identify system testing and Y2K certification as appropriate.

Resource Plan for Operating in Contingency Mode

Address all of the necessary resources (e.g. staff, materials, supplies, temporary hardware and software, facilities, etc.) required to successfully operates in the contingency mode. Additionally, the resource plan should include an estimated schedule.

Training requirements for operating in contingency mode

Identify essential training requirements to ensure that personnel are capable of successfully implementing the contingency operations.

Contingency Mode Closeout

Describe the activities and procedures to close out the contingency operation such as the problem, problem resolution, and date of resolution, and notification requirements (e.g., management, Year 2000 Project Office).

Hanford Year 2000 Business Continuity Plan

ATTACHMENT 3: ASSURANCE OF MISSION-CRITICAL SYSTEM CONTINGENCY PLAN COMPLETION

System Name: _____ System Owner: _____

The system Owner has documented completion of the following:

_____ Date final mission-critical system Contingency Plan was completed.

Based on the information and documentation presented, the undersigned acknowledges that a Contingency Plan has been prepared, tested and has addressed all Y2K – related risks and provides for the continuity of operations for the function performed by the mission-critical system. Each mission-critical system should have this form completed.

Contractor Representative Date

Local Y2K Project Coordinator Date

HQ/Field Office or Site Manager Date

Please retain this form for your files, and provide a copy, along with the completed mission-critical system Contingency Plan and other supporting documentation, to the Site Manager. Copies of Attachment 3 should be forwarded to the DOE Chief Information Officer (MA-4). Documentation should be made available to the appropriate Program Secretarial Officer(s) (PSO) and to the Office of the Chief Information Officer, if requested.

Direction for Business Continuity and Mission-Critical Contingency Planning, Revision 9
REVISED DRAFT: December 22, 1998.