ATTACHMENT 1

Action Plan to address DNFSB Concerns
Associated with April 19, 2002 Letter

1.0 Background

The Plutonium facility (Building 332) was designed for the conduct of research and development (R&D) projects using radio-nuclides in primary support of nuclear weapons dismantlement/stockpile stewardship, plutonium and uranium disposition and chemical, metallurgical and physical properties of plutonium and uranium. The key control to prevent a radiological airborne release (i.e., to provide confinement) during postulated accident scenarios that might affect the public is the building's structure. In addition, based upon assumptions such as the amount of material at risk, energy available for dispersion, and the leak paths, the ventilation system is relied upon in certain postulated accident scenarios to provide confinement. The current Building 332 (B-332) Safety Analysis Report (SAR) states that room ventilation system exhaust fans, and certain active components (fire damper actuators) in the fire protection systems rely on emergency power. The Emergency Power System (EPS) consists of (1) two diesel-engine emergency generator sets, (2) five automatic transfer switches (3) one uninterruptible power supply and (4) systems that directly support the EPS.

1.1 Letter from the Board

During November 1999, the DNFSB staff reviewed the design of the electrical distribution system for B-332[1]. The emphasis of that review was on the Emergency Power System, which was designated as safety-class. Issues were identified as a result of this review. The Laboratory prepared a corrective action plan during May 2000[2] and updated that plan during June 2000[3]. A progress report was provided by LLNL in March of 2001[4]. The DNFSB staff conducted follow-on visits associated with electrical systems during September 2000 and March 2002.

On April 19, 2002, the DNFSB issued a letter to the Secretary of Energy about concerns associated with the Lawrence Livermore National Laboratory Emergency Power System[5]. A summary of the interpretation of the concerns identified in the DNFSB letter include the following:

1. Lack of identification/specification of requirements. The role of current codes and standards in evaluating system adequacy has not been defined. The safety function, functional requirements and performance criteria of the existing B-332 Emergency Power System are not adequately identified.

2. Lack of a documented/defined technical basis.

3. Lack of identification of vulnerabilities.

4. Corrective actions associated with the B-332 Emergency Power System have not been timely and prioritized by the NNSA and LLNL in a manner that is consistent with DNFSB's assessment.

5. Requirements associated with the design of safety class electrical power systems are not contained in the LLNL contract and flow-down of guidance contained in DOE

Implementation Guide 420.1-1 has not been clearly defined since the Order does not apply to existing systems.

2.0 Resolution of Concerns

LLNL and NNSA have developed an action plan to address the concerns raised by the DNFSB that are noted in Section 1.1 of this plan. This section identified the actions necessary to address the DNFSB concerns. Each concern is described, the intended course of action is noted, the specific safety improvement(s) expected is addressed (specific commitments with dates), and responsibilities and deliverables are identified. The flow of work to implement this action plan is outlined in Figure 1. The scheduling of the work activities is presented in Figure 2.

2.1 Key Concerns and Associated Actions

2.1.1 Concern #1 – The requirements of the existing B-332 Emergency Power System are not adequately identified and specified for a safety class system. The role of current codes and standards in evaluating system adequacy has not been defined. The safety function, functional requirements and performance criteria of the existing B-332 Emergency Power System are not adequately identified.

During 1998-1999, LLNL, OAK and DOE-HQ personnel actively worked to develop Work Smart Standards for the site, which were included in the DOE/UC contract W-7405-ENG-48, as modified. These standards addressed electrical system requirements for new facilities or modifications but did not address the existing operating facilities. No back-fit policy or standard was developed for existing safety-class electrical systems. Requirements for existing electrical systems have not been identified for the system design or for justification of deviations.

A commitment is made in this plan to determine what are the appropriate standards and requirements for an existing safety class emergency power system. The existing B-332 SAR has limited discussion and derivation of functional requirements and performance criteria.

Commitment (a):	Establish a Standards Identification Team (SIT) to identify the standards and requirements for the existing safety class Emergency Power System.
Responsibility:	NNSA-OAK Assistant Manager for National Security and LLNL Change Control Board Chairperson.
Deliverable:	List of standards and requirements for design and operation of existing safety class emergency power.
Due Date:	October 1, 2002
Commitment (b):	Establish a Standards Identification Team (SIT) to identify the requirements for a Back-fit Policy at LLNL for existing safety class Emergency Power System.
Responsibility:	NNSA-OAK Assistant Manager for National Security and LLNL Change Control Board Chairperson.
Deliverable:	A back-fit policy for LLNL safety class electrical power systems.
Due Date:	January 31, 2003

Commitment (c):	Submit the 10CFR830 Subpart B compliant B-332 Safety Analysis Report and Technical Safety Requirements to reflect current EPS configuration including revised functional requirements and performance criteria (including equipment qualification).
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Revised SAR/TSRs.
Due Date:	October 1, 2003

2.1.2 Concern #2 – Lack of a documented/defined technical basis.

In 1995, the B-332 Safety Analysis Report[6] (SAR) was developed as a compilation of efforts associated with the Basis for Interim Operations and other safety analysis documents. System design documents were not developed for safety systems. In the current SAR, the Emergency Power System was designated as safety class, because the ventilation system needed electrical power to perform its safety function to limit consequences of some analyzed accident scenarios. The corresponding Safety Evaluation Report[7] identified that the facility had been designed and constructed prior to the issuance of DOE Order 6430.1A, General Design Criteria. Configuration management controls did not keep current with changes in the facility. Unlike a new construction project in which the Preliminary SAR would document the design basis for the facility, the SAR needed a reconstituted design basis that involved validating current systems configuration and accident analyses based on the system, as it currently existed. Several systems, structures and components including the Emergency Power System for which the design basis was unknown had to undergo an effort to assure that the assumptions of operability of equipment were valid and the descriptions were accurate. However, documentation to reconstitute the design basis was not completed. At that time an upgrade to the Emergency Power System was underway. The emergency diesel generators and automatic transfer switches were part of the upgrade. Two key exceptions to DOE Order 6430.1A were identified in the SAR for the Emergency Power System as follows:

1. The criteria specifying that an alternate primary feeder shall be in ready-standby for use by an automatic transfer switch.

2. Redundant safety-class electrical systems must be protected and separated to prevent a common external event from causing a failure of redundant systems.

In January 1997, a DOE-Headquarters Defense Programs team[8] conducted a site visit to document the Department's understanding of the circumstances surrounding the issues concerning the B-332 Emergency Power System, its design capability to support the building ventilation systems during postulated accidents and the associated safety analysis. The conclusion from this visit was that LLNL should reanalyze key accidents in its SAR. The analysis was not to defend the adequacy of the existing design, but to develop a solid technical understanding of potential accident scenarios and appropriate safety functions and to establish a sound and defensible technical safety basis for B-332. Design basis documentation was not addressed.

Throughout these different efforts, the design basis was not brought into current configuration for the emergency power system, but instead individually assessed with each modification. The acceptance of risk had previously been based upon higher-level reviews of single point failures rather than detailed inspection.

Commitment (d):	Develop current system design description documentation for use in the Institutional Review of the Emergency Power System in B-332.[1]
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	System Design Description for the Emergency Power System in B-332.
Due Date:	October 1, 2002
Commitment (e):	Update drawings (including labeling), calculations, differentiate safety-class from non-safety class loads to reflect the current installed configuration of the B-332 Emergency Power System.[1]
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Letter stating that the supporting information for the system design description reflects current configuration and analysis has been completed.
Due date:	October 1, 2002

2.1.3 Concern #3 – Lack of identification of vulnerabilities.

To better understand the gap-related vulnerabilities associated with the B332 Emergency Power System (EPS), an Institutional Review (IR) shall be conducted using a DNFSB Recommendation 2000-2 Phase II type CRAD. A gap analysis comparing the B-332 EPS to the newly modified Work Smart Standards (WSS) for the existing safety class EPS and gaps identified in the Institutional Review will then be performed. Once the gaps are identified, a Vulnerability Assessment shall be conducted to understand system vulnerabilities associated with reliability, operability and maintainability.

Commitment (f):	An Institutional Review (IR) shall be conducted on the B-332 Emergency Power using a DNFSB Recommendation 2000-2 Phase II type CRAD.
Responsibility:	NNSA Deputy Administrator for Defense Programs.
Deliverable:	Written report that identifies the reliability, operability and maintainability adequacy of the system.
Due Date:	Commence October 1, 2002. Final Report January 31, 2003
Commitment (g):	Perform a gap analysis comparing the B-332 Emergency Power System to the newly modified Work Smart Standards (WSS) for the existing safety class EPS and gaps identified in the Institutional Review.

[1] These commitments are essential to having a substantive, meaningful evaluation of the current EPS against the applicable standards to determine the gaps along with accurately assessing the risks.

Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Written report (gap analysis).
Due Date:	February 28, 2003

Commitment (h):	A vulnerability assessment shall be conducted on the B-332 EPS to identify system vulnerabilities associated with reliability, operability and maintainability.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Written report that identifies the vulnerabilities of the B-332 EPS.
Due Date:	May 31, 2003

2.1.4 Concern #4 -- Corrective actions associated with the B-332 EPS system have not been timely and prioritized by the NNSA and LLNL.

The Vulnerability Assessment and Gap Analysis will be evaluated considering the safety benefit with the associated risk in implementing, programmatic impact, and cost to allow the development of a prioritized list of options. The funding of selected options and the scheduling of the implementation of necessary actions will follow.

Commitment (i):	Develop Corrective Action Options and recommendations.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Letter that identifies the Corrective Action Options with recommendations.
Due Date:	June 30, 2003

Commitment (j):	Options selected by NNSA.
Responsibility:	NNSA-OAK Assistant Manager for National Security and NNSA Deputy Administrator for Defense Programs.
Deliverable:	Letter that identifies the selected options.
Due Date:	July 31, 2003

Commitment (k):	Incorporation of NNSA selected Corrective Action Options and discussion of risks into B-332 SAR/TSRs. Mitigation of gaps until options are implemented will be described.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	10CFR830 Subpart B compliant SAR/TSRs.
Due Date:	October 1, 2003

2.1.5 Concern #5 -- Requirements associated with the design of safety class electrical power systems are not contained in the LLNL contract and flow-down of guidance contained in DOE Implementation Guide 420.1-1 has not been clearly defined.

DOE Order 420.1 specifically states in Section 4.1.1.2, Design Requirements, that *Facility safety class electrical systems shall be designed to the basic approach outlined in Section 5.2.3 (Electrical) of "Implementation Guide for Nonreactor Nuclear Safety Design Criteria and*

Explosives Safety Criteria." The DOE Order 420.1 CRD does not contain these requirements. Additionally, the LLNL contract does not contain the standards listed in Section 5.2.3 of the DOE Guide 420.1-1.

DOE Guide 420.1-1 describes necessary features of safety-class electrical power systems. The Guide goes on to state that safety-class electrical power must be designed against single-point failure in accordance with the criteria in Section 5.1.1.2 of the Guide and redundancy requirements for electrical systems should be analyzed on a case-by-case basis. The Guide also states that the environmental capability of safety-class electrical equipment must be demonstrated by testing, analysis, and operating experience or by a combination of these methods in accordance with Section 5.1.3 of the Guide. Also there is discussion in the Guide about Safety Class 1E requirements for commercial nuclear power reactors may not be directly applicable to the safety-class category defined for nonreactor nuclear facilities. These standards however contain useful and significant information that should be considered. Table 5.5 of the Guide lists a minimal set of national codes and standards that should be addressed for safety-significant and safety-class electrical systems.

During 1998-1999, LLNL, OAK and DOE-HQ personnel actively worked to develop Work Smart Standards for the site. These standards addressed electrical system requirements for new facilities or modifications but did not address the existing operating facilities. A commitment is made in this plan to determine what are the appropriate standards and requirements for the existing safety class emergency power system at LLNL. Additionally the list of standards and requirements for commercial nuclear power reactor safety-class emergency power systems will need to be reviewed to determine if they need to be fully incorporated into the DOE-UC contract (W-48) as part of Appendix F Work Smart Standards. Finally the flow down of processes, mechanisms, codes and standards contained in DOE Guide 420.1-1 need to be reviewed to ensure that appropriate contractor documents exist consistent with the Guide, and that there is justification for any alternative mechanisms used.

Commitment (1):	Following development of WSS for the existing safety class emergency power systems (Commitment 4.1.1.a), Contract W-48 will be revised to reflect any resulting new standards.
Responsibility:	NNSA-OAK Assistant Manager for National Security and LLNL Chairman of the Change Control Board.
Deliverable:	Revised WSS in Contract W-48 for the existing safety class emergency power system.
Due Date:	February 1, 2003

3.0 Current EPS Reliability Upgrade Projects

Several upgrade projects are underway or have occurred in B-332 specifically targeted at improving the performance and reliability of the emergency power system. Efforts are currently underway to remove single-point failures in 13.8kV normal power supply to reduce challenges to the B-332 Emergency Power System in response to concerns raised in February 2000 DNFSB letter[9]. In addition, projects are proceeding that will mitigate the potential single point failures associated with both ATS-07 and ATS-10. The workflow for these three safety upgrade projects is

presented in Figure 3. Projects recently completed have eliminated two common mode failure mechanisms (i.e., water pipe break and forklift/vehicle impact) associated with the Emergency Power Automatic Transfer Switch (ATS) Banks. Other implemented EPS safety upgrades include the replacement of the ATSs and associated cabling, replacement of the Emergency Motor Control Centers and associated cabling, implementation of the Safety Class Breaker Maintenance Program, and installation of a new Uninterruptible Power Supply (UPS). These actions were based on an assessment of the B-332 EPS vulnerabilities performed at a higher level, rather than to the detail of panel load and feeders. Vulnerabilities may exist within components such as the relays, cabling, non-safety loads connected to safety busses, equipment qualification, and independence of circuitry. Once vulnerabilities are defined, they will be evaluated as described in 2.1.3 and 2.1.4 using a graded risk-based approach to determine the appropriate course of action. Options will be developed by LLNL and provided to NNSA to make selection on the best approach.

Commitment (m):	Replace the T500 transformer.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	Upgraded T500 transformer and separate transformer safety loads from non-safety loads.
Due Date:	May 21, 2004

Commitment (n):	Mitigate the single point failure mode associated with ATS-10.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	ATS-10 feeds Motor Control Center (MCC) E410A3. This MCC services Safety Class Loads in Increment 3 including exhaust fans FFE 1000 and 2000. The deliverable is the installed circuitry and Kirk Keys to allow temporary generator service to MCC E410A3.
Due Date:	January 31, 2003

Commitment (o):	Mitigate the single point failure mode associated with ATS-07.
Responsibility:	LLNL NMTP Program Leader.
Deliverable:	ATS-07 provides power to the Safety Class systems from the emergency diesel generators. It is a single point of failure. The deliverable is an installed, manually switched circuit, which bypasses ATS-07 and provides generator power to Safety Class loads in the event of a catastrophic failure of ATS-07.
Due Date:	March 14, 2003

4.0 Status Reports and Briefings

Periodic status reports and briefings will be provided to the NNSA OAK and Headquarters, as well as to DNFSB. These reports and briefings will describe Action Plan progress, products, and next steps. It is anticipated that they will also provide a forum for receiving feedback.

Commitment (p):	Status report to OAK and NNSA HQ management on progress, status and issues.
Responsibility:	NMTP Program Leader.
Deliverable:	Written report to OAK and NNSA HQ.

Due date:	October 1, 2002, January 31, 2003, May 31, 2003 and October 1, 2003
Commitment (q):	Presentation to DNFSB on status of the action plan in response to the April 19, 2002 letter.
Responsibility:	NNSA-OAK Assistant Manager for National Security and NNSA Deputy Administrator for Defense Programs.
Deliverable:	Briefing with DNFSB.
Due date:	August 2002, February 2003 and August 2003

It should be noted that the schedule described in the Action Plan was developed prior to receipt of the agenda for the DNFSB staff review currently scheduled for mid-August. Each such DNFSB staff review of B332 during the period of this Action Plan will impact the schedule presented by one or two weeks, depending on scope of the review.

5.0 References

(1) M.K. Hooper, *Letter from J.Conway to General Gioconda*, December 21, 1999, with attached November 23, 1999 DNFSB Staff Issue Report, January 6, 2000.

(2) A.A. Garcia, *LLNL Response to DOE-OAK Request to Address Issues Identified in the DNFSB Staff Issue Report dated 11/23/99*, February 29, 2000.

(3) J.A. Sefcik, *Submission of Updated Corrective Action Plan for DNFSB Staff Issue Report*, June 19, 2000.

(4) J.A. Sefcik, *Progress on Corrective Action Plan for DNFSB Staff Issue Report*, March 22, 2001.

(5) J.T. Conway Letter to The Honorable Spencer Abraham, April 19, 2001.

(6) UCRL-AR-119434 Volumes 1-2, Revision 0, *Defense and Nuclear Technologies Directorate Plutonium Facility ---Building 332 Safety Analysis Report*, January 1995.

(7) D. Eddy, DOE *Safety Evaluation Report for the Lawrence Livermore National Laboratory Plutonium Facility (Building 332)*, March 6, 1995.

(8) Kendall, R., *LLNL Building 332 Emergency Power System Safety Basis and Consequences of Failure*, February 1997.

(9) M.B. Whitaker, JR., *Forwarding Technical Concerns on the Electrical Distribution System at Lawrence Livermore National Laboratory*, February 25, 2000.

6.0 Acronyms and Abbreviations

B-332	Building 332
CRD	Contractor Requirements Document
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
EPS	Emergency Power System
FY	Fiscal Year
HQ	Headquarters

IR	Institutional Review
LLNL	Lawrence Livermore National Laboratory
NMTP	Nuclear Materials Technology Program
NNSA	National Nuclear Security Administration
OAK	Oakland Operations Office
R&D	Research and Development
SAR	Safety Analysis Report
SEMI	Safety and Emergency Management Inspection
SIT	Standards Identification Team
TSR	Technical Safety Requirement
UPS	Uninterruptible Power Supply
WSS	Work Smart Standards

Work Flow for B332 EPS Action Plan

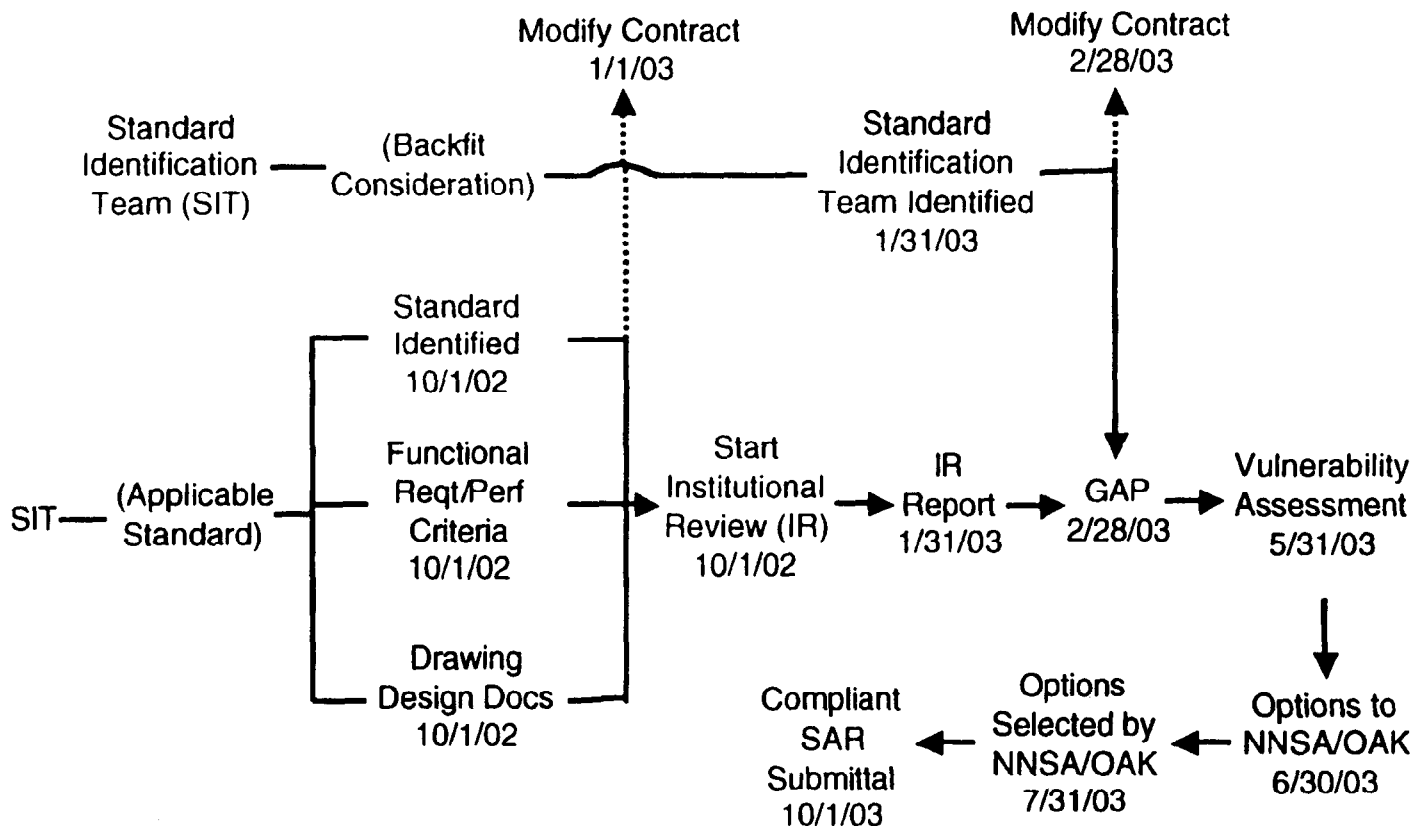
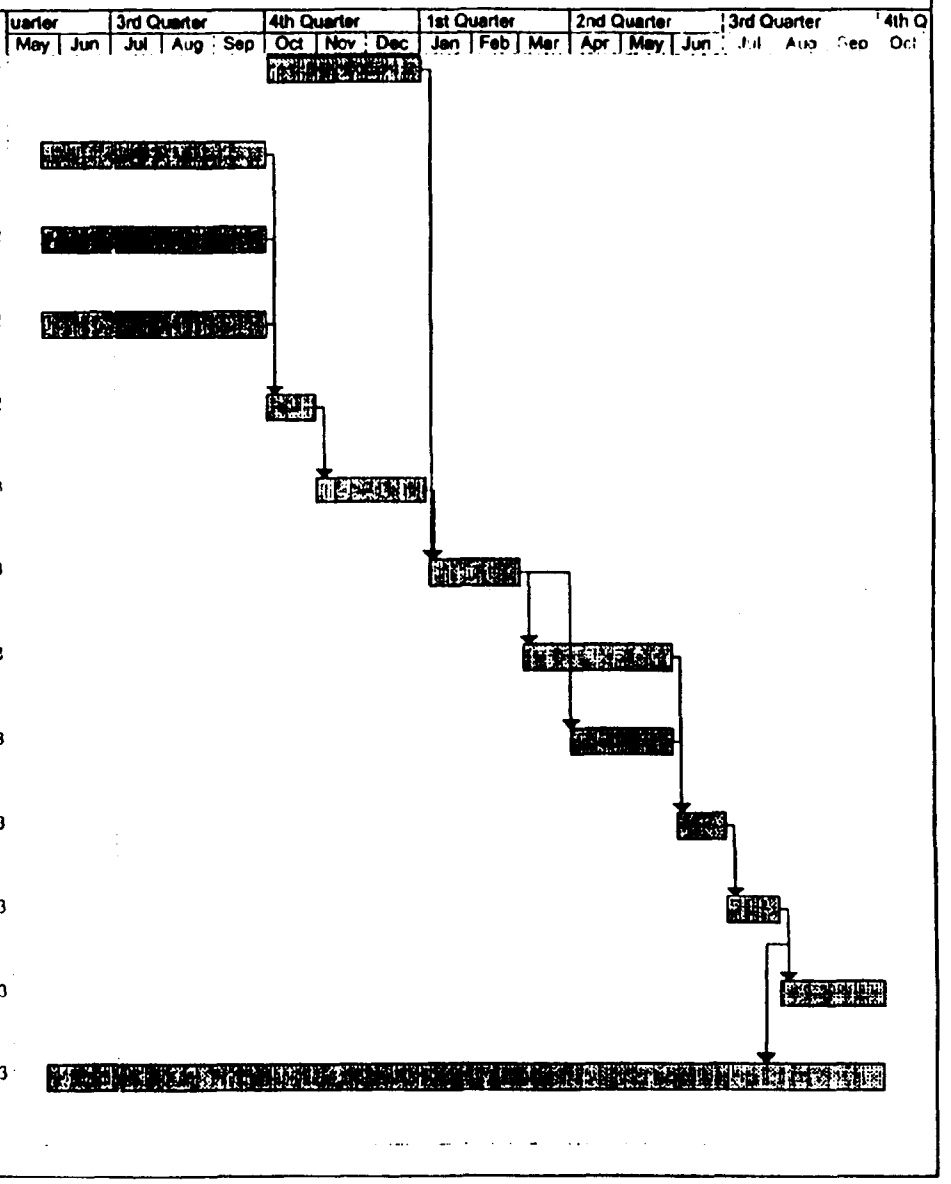


Figure 1

Schedule of Work Activity for B-332 EPS Action Plan
Figure 2

ID	Task Name	Start	Finish
1	Standards Identification Team (SIT): Develop Standard for Backfit	Thu 10/3/02	Wed 1/1/03
2	SIT: Develop Standard for existing emergency power system (EPS)	Tue 5/21/02	Tue 10/1/02
3	Evaluate B332 EPS Functional Requirements/Performance Criteria	Tue 5/21/02	Tue 10/1/02
4	Prepare Drawings & Design Documents for EPS	Tue 5/21/02	Tue 10/1/02
5	Compare installed system to Standard	Wed 10/2/02	Wed 10/30/02
6	Perform Institutionalized review	Thu 10/[illegible]/02	Fri 1/3/03
7	Perform Gap Analysis	Mon 1/6/03	Fri 2/28/03
8	Perform Vulnerability Assessment	Mon 3/3/03	Fri 5/30/03
9	LLNL to develop options	Mon 3/31/03	Fri 5/30/03
10	Provide Options to NNSA/OAK with recommendation	Mon 6/2/03	Mon 6/30/03
11	NNSA/OAK Selects Option	Tue 7/1/03	Thu 7/31/03
12	Develop Plan to Implement Options	Fri 8/1/03	Wed 10/1/03
13	Submit 10CFR830 Compliant SAR to NNSA/OAK (including mitigation until options are implemented)	Tue 5/21/02	Wed 10/1/03



Work Flow for B332 Equipment Upgrade

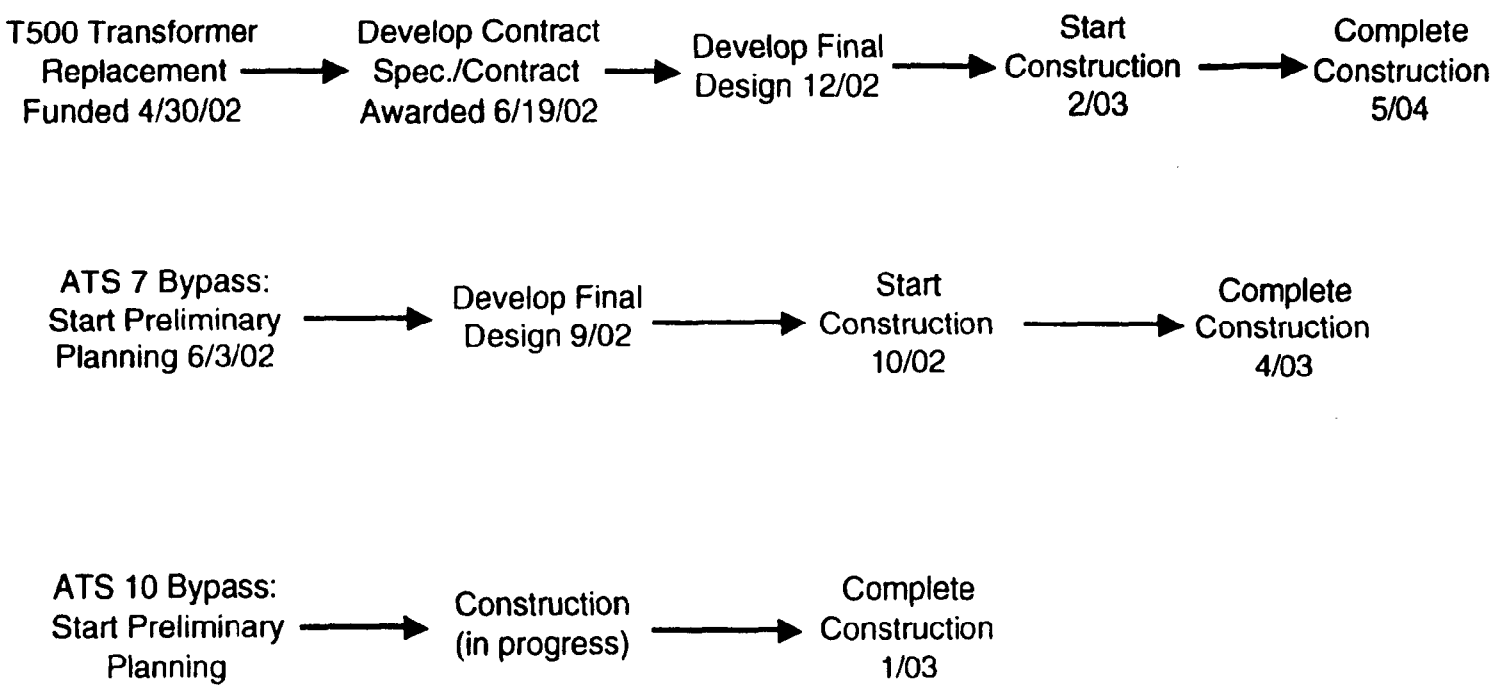


Figure 3