U.S. Department of Energy
Office of Inspector General
Office of Audit Services

# Audit Report

## Management Controls over Selected Departmental Critical Monitoring and Control Systems

OAS-M-05-06

June 2005

**Department of Energy**
Washington, DC 20585

June 3, 2005

MEMORANDUM FOR THE ASSOCIATE ADMINISTRATOR FOR MANAGEMENT AND ADMINISTRATION, NNSA

PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR FOSSIL ENERGY, FE-1

DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE, SP-1

ADMINISTRATOR, WESTERN AREA POWER ADMINISTRATION, WAPA

FROM: George W. Collard
Assistant Inspector General for Audit Operations
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "Management Controls over Selected Departmental Critical Monitoring and Control Systems"

BACKGROUND

The Department of Energy's overarching mission is to enhance the national, economic, and energy security of the United States. In pursuit of that mission, the Department and its contractors maintain and operate sophisticated information systems to monitor and control activities essential to protecting the nation's critical infrastructure and the public. Some of these systems manage the flow of electricity and emergency oil supplies, while others help secure access to highly sensitive facilities, information, and materials. Prolonged disruptions to these critical systems could impair the Department's ability to continue essential operations.

As noted in our report on *The Department's Continuity Planning and Emergency Preparedness* (DOE/IG-0657, August 2004), planning for continuity of operations and preparing for emergencies is essential to ensuring the continued operation of critical Department activities in the event of disaster. Assessments of risks and mitigation strategies are critical to such planning efforts and enhance the ability of organizations to maintain operational capability or quickly recover from service interruptions. Because of the importance of such systems, we initiated this audit to determine whether selected

Printed with soy ink on recycled paper

critical monitoring and control systems could continue operation in a crisis and/or had the ability to be restored with minimal disruption and information loss.

## RESULTS OF AUDIT

The Department could not ensure that selected critical monitoring and control systems could continue or resume operation with minimal disruption and information loss in the event of an emergency. Specifically, management did not always assess risks or take adequate steps to mitigate foreseeable risks. For example, for the six systems we evaluated:

- Two systems that controlled access to critical facilities and information and another used to control the distribution of energy resources did not have complete risk assessments that fully analyzed the likelihood and impact of natural disasters or human errors; and,

- Necessary steps to mitigate foreseeable risks – including the formulation of comprehensive contingency plans, establishment of secondary systems, and adequate protection measures for backup information – had not been completed for five of the systems reviewed.

Sufficient plans or mitigation strategies were not in place because the Department, despite Federal requirements, had not implemented a comprehensive risk management process. Without a thorough risk management process, the Department may be unable to sustain operations or recover from systems interruptions caused by disasters or other problems. As demonstrated by the 2003 Northeast power blackout, the inability to promptly recover from system-related problems has the potential to cause cascading system failures and widespread service interruptions.

Subsequent to our field visits, management at each of the sites informed us that they had either initiated or completed actions to identify and mitigate risks. For example, sites had initiated or completed certification and accreditation of the systems discussed in this report or had taken other actions to mitigate risks. While such actions are promising, they were not completed until after our site visits and have not been reviewed for accuracy or completeness. The Department's ongoing independent validation and verification of such actions, as well as our testing as required by the *Federal Information Security Management Act*, however, has demonstrated problems with the completeness and quality of similar system certification efforts. For these reasons and for others addressed in our report, we believe that additional action is necessary in this important area. In that connection, we have made several recommendations designed to improve the overall security of the Department's critical monitoring and control systems.

## MANAGEMENT REACTION

Management generally concurred with our findings and recommendations. The Chief Information Officer (CIO) stated that the program offices have made significant progress

in addressing and correcting the weaknesses we identified. Also, the CIO has established an overall goal that all Department systems be certified and accredited by September 2005. Where appropriate we have incorporated Management's comments into the body of this report. Management's comments are included in their entirety in Appendix 3.

Attachment

cc: Chief of Staff
Chief Information Officer

# REPORT ON MANAGEMENT CONTROLS OVER SELECTED DEPARTMENTAL CRITICAL MONITORING AND CONTROL SYSTEMS

## TABLE OF CONTENTS

### Protecting Critical Monitoring and Control Systems

Details of Finding .....1

Recommendations.....5

Comments .....6

### Appendices

1. Objective, Scope, and Methodology.....9

2. Prior Reports .....11

3. Management Comments .....13

# PROTECTING CRITICAL MONITORING AND CONTROL SYSTEMS

## Ensuring Continuation or Restoration of Essential Operations

The Department of Energy (Department) could not ensure that it could continue operations or quickly restore selected critical monitoring and control systems in the event of an emergency. Specifically, management had not fully assessed risks or taken adequate steps to mitigate the foreseeable risks confronting the six critical monitoring and control systems we reviewed.

### Risk Assessments

Management had not fully assessed the risk and cost-benefit of risk mitigation strategies for three of the six systems we reviewed, including Argus which is a system deployed at a number of sites to control access to facilities that house critical information and nuclear materials. To manage risk, the *Federal Information Security Management Act* requires agencies to assess, mitigate, and periodically reevaluate risks and security measures for all major systems. Risk assessments enable management to identify threats, vulnerabilities, and the likelihood of adverse actions or potential consequences. Specifically, management had not:

- Conducted a comprehensive risk assessment for Argus at Lawrence Livermore National Laboratory (Livermore). While program officials had addressed the risk of the system and of its network not being available, they had not identified and mitigated risks posed to the system by natural disasters, environmental hazards, or human error. For example, the risk of human error was increased because an administrator was responsible for both reviewing vulnerability scans and implementing corrective actions to address identified vulnerabilities. To the site's credit, management took action to correct this problem when we brought it to their attention.

- Fully analyzed the cost and benefit of strategies to mitigate identified threats and vulnerabilities posed to the Distributed Control System which controls the emergency oil flow at the Strategic Petroleum Reserve. For example, at the time of our site visit, management had not completed its

assessment of the likelihood of exploitation of identified vulnerabilities nor the impact of such exploitation on the system and its energy resource mission. Consequently, management could not fully assess the probability and consequence of vulnerabilities being exploited or evaluate the cost and benefits of eliminating such issues. Subsequent to our field visit, management informed us that they had completed a risk assessment that included risk mitigation action plans.

- At the time of our site visits, officials had not completed a documented risk assessment to identify and evaluate potential system threats and vulnerabilities for the Argus system that is used to control access to the Department Headquarters (Headquarters).

Risk Mitigation

Management did not take necessary actions to mitigate foreseeable risks associated with critical monitoring and control systems. Specifically, management had not fully developed and tested contingency plans for three of the six systems to ensure that emergency situations would be effectively managed. Also, it did not ensure it could recover from an incident by protecting system backup capabilities from the same risks posed to the primary systems. Four of the six systems either had their backup systems and/or backup software co-located with the primary system or had not provided backup capability to control critical processes during an emergency situation. For example:

- The Western Area Power Administration's (Western) Supervisory Control and Data Acquisition system (SCADA), which helps control the flow of electricity to a regional power grid, had its backup copies of system software and data co-located with the primary system, in part because its contract for off-site storage had lapsed. It also had its backup system co-located with the primary system. The Livermore Argus system also had backup copies of system software

and data co-located with the primary system. In addition, contingency plans for recovering mission capability for both the Western and Livermore systems had not been completed or tested. Near the end of our audit we learned that Western had purchased and was configuring a secondary control system that management planned to locate off-site. Also, subsequent to our review, Western indicated that it had arranged to ship data backups to an off-site storage facility on a regular basis.

- The Savannah River Site's Distributed Control System used to control the flow of tritium at its processing facility did not have a backup system and did not have a plan that fully addressed recovery of system capability.

- The Strategic Petroleum Reserve Distributed Control System, used to control the flow of oil to emergency reserves, had its primary and backup system located in the same room. The system contingency plan at the Strategic Petroleum Reserve was limited to procedures for obtaining a manual replacement system in the event of system failure, and did not address the susceptibility to failure caused by common disasters due to maintaining primary and backup systems in the same control room. Had the primary and backup systems been adequately separated, it may have eliminated the need to adopt manual methods – a process described as costly by a site engineer – in the event of a localized disaster.

**Risk Management**

Site management had not sufficiently considered and periodically evaluated the risk that critical monitoring and control systems we reviewed would become inoperable and unable to be restored in a timely manner. For example, five of the six systems reviewed had not been certified and accredited (C&A) for operation according to National Institute of Standards and Technology (NIST) guidance at the time of our site visits (only the Savannah River Site had certified and accredited the Defense Waste Processing Facility's Distributed Control System). C&A represents senior management's decision to authorize the system for

operation and requires management to explicitly accept the risk of operating the system based on an agreed upon set of security controls. According to NIST, systems cannot be properly certified and accredited unless management ensures that it completes a risk assessment, security plan, contingency plan, and necessary mitigating controls. In commenting on a draft of our report, management officials stated that they had begun or completed implementing a comprehensive risk management process, to include C&A of systems and other mitigating actions.

Furthermore, the Department had made only limited use of its own internal experts in evaluating the risks pertaining to critical monitoring and control systems. The Department established a group of energy infrastructure control system experts at Sandia National Laboratory that have provided advice to private sector utilities regarding critical control systems. These experts told us that they had received very few internal requests to utilize their expertise. Of the sites we reviewed, only the Strategic Petroleum Reserve availed themselves of these experts. Officials at one site we visited stated that they were not aware that these experts were available. Had their services been utilized, many of the weaknesses we identified may have been disclosed and corrected. After our field work was complete, management officials told us that they intend to utilize Departmental expertise in the future where appropriate.

**Critical Infrastructure and Public Safety**

Critical monitoring and control systems were vulnerable to disruptions due to disasters or other emergencies. Assessing and mitigating risks to these systems may help prevent extended system shutdowns that could lead to the wide-scale disruptions to electricity grids, the inability to maintain controlled access to critical information and nuclear materials, or the use of costly alternatives to provide emergency energy supplies in the event of a national crisis.

The lack of adequate backup systems and contingency planning were recently highlighted as part of the cause of the August 2003 blackout in the northeast portion of the United States. Key monitoring systems failed, thereby preventing electricity control operators from detecting a short circuit in the grid, resulting in a cascading power failure across the northeastern United States. A joint United States and Canadian task force investigating the blackout also noted that it was caused in part by failure to conduct multiple contingency and extreme condition assessments and to have backup monitoring tools available after the primary alarming/monitoring systems failed.

## RECOMMENDATIONS

To ensure that the Department's critical monitoring and control systems are able to continue operation in the event of emergencies, we recommend that the Associate Administrator for Management and Administration, National Nuclear Security Administration; the Principal Deputy Assistant Secretary for Fossil Energy; the Director, Office of Security and Safety Performance Assurance; and the Administrator, Western Area Power Administration ensure that critical monitoring and control system owners:

1. Implement a comprehensive risk management process for its critical monitoring and control systems. This process should include:

    a. Periodically assessing and mitigating risk to these major systems, including the completion of risk assessments, contingency plans, and certification and accreditation of systems;

    b. Ensuring that backup systems and media are located a sufficient distance from the primary system to facilitate system recovery, to include consideration of off-site locations; and,

2. Take advantage of Department expertise to periodically evaluate and strengthen management controls over critical monitoring and control systems.

## MANAGEMENT REACTION AND AUDITOR COMMENTS

Management generally concurred with the report's overall conclusion and recommendations, but offered clarifying remarks or disagreed with some of our conclusions regarding specific systems.

Proposed and stated actions are generally responsive to our recommendations. Based on management's comments, we modified our report where appropriate and deleted a recommendation "to evaluate the need for remote system operation capability." We have also made a number of other technical corrections to our report to address management's comments.

In reference to specific site comments, management reaction and the auditor responses follow.

Livermore Argus System

Management stated that while risk mitigation is a concern, they considered Livermore's compensatory measures to be adequate. They also noted they maintain this system's operational software and backup tapes in a separate area where it is readily available.

Management acknowledged that, despite a growing need, a formal, comprehensive and documented risk assessment has not occurred. We believe that in the absence of such an analysis, management can not be assured that all risks have been fully assessed and properly mitigated for these systems. We do not agree that having Livermore Argus backup data in an area separate from the live Argus system is sufficient, since we found that the separate area is adjacent to the room housing the live Argus system. Thus, the backup tapes may be subject to the same localized disaster as primary Argus system, such as flooding or fire.

Headquarters Argus System

Management indicated that based on an assessment of the impacts of adversary data theft at another site's Argus system, the impacts on the Headquarters system would be minimal since it operates on a closed Local Area Network. Officials also stated that they have a "fail-over" scheme to mitigate loss of functionality at either the Forrestal or the Germantown facility by utilizing the other site's host

computer in the event of a system failure. They also noted that impacts due to human error are mitigated by providing a limited number of trained individuals and a well trained protective force to solely perform critical system functions and restore the Headquarters' system's access control system should it be rendered inoperative.

Nonetheless, a Headquarters official told us that the link between the two sites was interrupted on more than an occasional basis. The Headquarters Argus "fail-over" scheme to mitigate loss of functionality at either the Forrestal or the Germantown facility does not address the fact that connectivity between the two sites is adversely affected when the main data link between the sites is disrupted.

Western's SCADA System

Management stated that the system was certified and accredited under independent review in compliance with NIST requirements and this information should be updated in the report's Risk Management section.

The Office of Inspector General does not agree with Western's assertion that the SCADA system had been certified and accredited in accordance with NIST requirements at the time of our review. The certification documentation we were provided and examined lacked various elements needed to be consistent with NIST guidance, such as the existence of contingency procedures should a failure of the SCADA system occur. Also, Western management officials told us that the certification and accreditation satisfied requirements of the North American Electric Reliability Council, not necessarily those of NIST.

Strategic Petroleum Reserve's
Distributed Control System

Management explained that the controllers, input/output modules, and the operator stations employ some form of redundant backup that supports the metric of 95 percent availability of systems [and] are all located in the same control room to provide seamless recovery from any equipment failure. Officials added that the backup for a total system failure is to manually operate the existing site

process equipment. They also noted that in conformance with design criteria, the functional specification for the system excluded the remote operability of the process equipment. They stated that operational and security concerns outweighed the potential benefits and that manual operation of the site's process equipment as a backup to total DCS failure is significantly less costly than providing for remote capability.

Management had no documented risk assessment or cost benefit analysis to support its decision to have the people, process, and technology related to this system located in the same control room and to rely on a costly manual process to recover in the event of a total system failure. We believe that Strategic Petroleum Reserve officials should have documented how they arrived at their conclusions and thus allowed management to make an informed decision regarding whether to accept the associated risks during the system accreditation process.

Management's comments are included in their entirety in Appendix 3.

**OBJECTIVE**

To determine whether selected critical monitoring and control systems could continue operation in a crisis and/or had the ability to be restored with minimal disruption and information loss.

**SCOPE**

The audit was performed between October 2003 and March 2005 at Department Headquarters, Washington, DC; Lawrence Livermore National Laboratory, Livermore, CA; Western Area Power Administration, Folsom, CA; Savannah River Site, Aiken, SC; and the Strategic Petroleum Reserve, New Orleans, LA. Specifically, we performed a comprehensive review of the agency's key processes for managing critical monitoring and control systems information technology resources.

**METHODOLOGY**

To accomplish our audit objective, we:

- Reviewed a sample of the critical monitoring and control systems as identified by Department officials and the Project Matrix Step One Report, dated August 2003;
- Reviewed applicable laws, regulations, guidance and best practices pertaining to managing information technology resources and initiatives. We also reviewed relevant reports issued by the Office of Inspector General and the Government Accountability Office;
- Reviewed the *Government Performance and Results Act of 1993* and determined if performance measures had been established for managing information technology resources;
- Reviewed numerous documents related to the management of critical monitoring and control systems, including information technology risk management and contingency planning documentation; and,
- Held discussions with program officials and personnel from the field sites.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objectives. We assessed significant internal controls and performance measures in accordance with the *Government Performance and Results Act of 1993* regarding the management of the Department's critical monitoring and control systems. We did not identify any performance measures specific to managing critical monitoring and control systems. However, the Office of the Chief Information Officer (OCIO) has begun tracking information on the number of systems that have been certified and accredited and have developed and tested contingency plans. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to accomplish our audit objective.

An exit conference was held with appropriate management officials on May 19, 2005.

## PRIOR REPORTS

### Office of Inspector General Reports

- *The Department's Continuity Planning and Emergency Preparedness* (DOE/IG-0657, August 2004). The report found five sites did not develop comprehensive plans to continue essential functions. Specifically, the sites had not fully identified essential functions or alternate facilities in case of emergency. Additionally, the Department did not have specific requirements for sites to validate the effectiveness of corrective actions addressing recognized preparedness weaknesses or to share complex-wide lessons learned about common problems. As a result, the Department may face increased risks to operations, employees, and surrounding communities during an emergency situation.

- *Electricity Transmission Scheduling at the Bonneville Power Administration* (DOE/IG-637, February 2004). The report outlined the results of an audit conducted to determine whether the Bonneville Power Administration (Bonneville) has a scheduling system in place to meet current and future transmission needs in an automated, deregulated environment. Bonneville's system for scheduling transmission transactions did not fully meet its needs in the current operating environment. Bonneville's management of the replacement system lacked a comprehensive project plan, and system development and implementation procedures. The effectiveness of the project management effort was hampered by the lack of standardized transmission contracts. Automated scheduling would enhance Bonneville's electrical transmission grid by allowing Bonneville to react more quickly to disruptive events, such as a May 2003 incident in which Bonneville exceeded the operating capacity of one of its transmission lines.

- *Planning for National Nuclear Security Administration Infrastructure* (OAS-B-03-02, May 2003). The report outlined the results of an audit conducted to determine whether the National Nuclear Security Administration's (NNSA) site plans provided accurate and useful data to aid in the prioritization of mission critical facility renovation and repair projects. The OIG concluded, in part, that NNSA site plans did not identify or prioritize the mission critical facilities and infrastructure in need of repair or refurbishment.

- *Cyber-Related Critical Infrastructure Identification and Protection Measures* (DOE/IG-0545, March 2002). The report outlined the results of an audit conducted to determine whether the Department had identified and developed protection measures for its critical cyber and related physical infrastructure assets. While the Department had initiated certain actions designed to enhance cyber security, it had not made sufficient progress in identifying and developing protective measures for critical infrastructures or assets. Even in light of the magnitude of the challenges it faces in this arena, the Department had not devoted sufficient resources to identifying and developing protective measures for cyber-related assets.

**Government Accountability Office (GAO) Reports**

- *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO 04-354, March 2004). GAO found that along with the increasing cyber threats to control systems, other factors such as standardized technologies with known vulnerabilities and increased connectivity increased the risk to these systems. They note that successful attacks on control systems could have devastating consequences, such as endangering public health and safety. Securing control systems poses significant challenges, including limited specialized security technologies. Without effective coordination of efforts to secure these systems, there is a risk of delaying the development and implementation of more secure systems to manage our critical infrastructures.

- *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors* (GAO-03-233, February 2003). GAO issued this report in response to a Congressional request to assess the pace and progress of certain Federal agencies (including the Department of Energy) and private sector Information Sharing and Analysis Centers in achieving certain objectives contributing to the protection of infrastructures critical to the nation. GAO concluded that although the agencies under review had taken some actions to implement critical infrastructure protection policy, they had not completed the fundamental step of identifying their critical infrastructure assets and the operational dependencies of these vital assets on other public and private assets.

**Department of Energy**
Washington, DC 20585

March 8, 2005

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR AUDIT OPERATIONS
OFFICE OF INSPECTOR GENERAL

FROM: ROSITA O. PARKES
CHIEF INFORMATION OFFICER

SUBJECT: Response to Office of Inspector General Draft Report on *Management Controls over Selected Critical Monitoring and Control Systems* (A04TG029)

We appreciate the opportunity to provide to you the consolidated comments from our Program Offices in response to your draft report on the subject audit. This memo contains Program Office comments and concerns on the draft report as well as details on corrective actions taken and planned target dates to incorporate your recommendations. All of the Program Offices have made significant progress since the audits were conducted, and except for a few minor concerns, they all agreed with the report's recommendations and have made efforts to adopt them where possible.

**Recommendation 1**

a. Periodic Assessments

The Fossil Energy (FE) Strategic Petroleum Reserve (SPR) has strengthened its implementation of the comprehensive risk management process for its distributed control system (DCS) for crude oil movement in accordance with requirements in current Department of Energy (DOE) Directives and applicable National standards. The DCS was certified and accredited on March 29, 2004. The SPR completed a four month vulnerability assessment in March 2004. The SPR also completed a risk assessment that complied with DOE Notice 205.9 *Certification and Accreditation Process for Information Systems*. The SPR will conduct periodic assessments of the DCS every three years or coincident with any major change to maintain certification and accreditation.

Over the life span of the National Nuclear Security Administration's (NNSA) Lawrence Livermore National Laboratory (LLNL) ARGUS system, which was certified and accredited by the Livermore Site Office (LSO) in September 2004, a formal, comprehensive and documented risk assessment has not occurred despite a growing need for one. While risk mitigation is a concern, LSO considers LLNL compensatory measures to be generally adequate. Based on an assessment of the impacts of adversary data theft or sabotage at another site's ARGUS system, the impacts on the Headquarters

Printed with soy ink on recycled paper

system would be minimal as it operates on a closed LAN. Headquarters' systems are housed in concrete facilities to meet the DOE Orders requirement for Central Alarm Stations and are therefore protected against a majority of, if not all, natural disasters.

In September 2004, the LLNL ARGUS Security Alarm and Access Control Systems (SAACS) was certified and accredited in accordance with the self-assessment process described in the National Institute of Standards and Technology (NIST) SP 800-26 *Security Self-Assessment Guide for Information Technology Systems* process. The Office of Security and Safety Performance Assurance later developed a SAACS Security Plan to address the assessment findings. Impacts due to human error are mitigated by providing a limited number of trained individuals and a well trained protective force to solely perform critical system functions and restore the Headquarters' system's access control system should it be rendered inoperative.

At the time of the audit, Western's Supervisory Control and Data Acquisition (SCADA) System was certified and accredited under independent review and in compliance with NIST requirements and should be updated in the report's Risk Management section. Western has since implemented risk assessment mitigation efforts and now uses documented Risk Management Life Cycle processes to document risk and mitigation plans that identify tasks, scheduled completion dates, and resources. In addition, there is a draft plan with milestones to complete the Continuity of Operations Plan for the Folsom Office, which includes critical business functions, remote system operations, and system recovery processes. Western also has documented SCADA System Disaster Recovery Plans.

The Office of Environmental Management (EM) would like to point out that although it is the cognizant Lead Program Secretarial Office at the Savannah River system, identified as the Distributed Control System for Tritium, NNSA actually owns and manages the site. Because the system is not part of EM's capital investment portfolio for IT systems, NNSA is responsible for the management of the system's risks and emergency operations. NNSA will implement a comprehensive risk management process for its critical monitoring and control systems and will take advantage of expertise to periodically evaluate and strengthen management controls over these systems.

b. Backup System/Media

DCS controllers, input/output modules, and the operator stations employ some form of redundant backup that supports the metric of 95 percent availability of SPR systems are all located in the same control room to provide seamless recovery from any equipment failure. The backup for a total DCS system failure is to manually operate the existing site process equipment. All backup media is currently located offsite.

NNSA interpreted Recommendation 1.b. to imply that all backup systems and media **must** be located off-site to facilitate system recovery, but believes that the intention

should be part and parcel of a comprehensive risk management strategy, including an appropriate cost/benefit assessment. NNSA does maintain its operational software and backup tapes containing current site configuration data within approximately 30 days in a separate area where it is readily available.

Western now performs systems backup in compliance with Western Policy 200.1, *Western Systems Backup and Recovery Policy*, to ensure that mission-critical SCADA data is backed up nightly and archives are adequately preserved and protected against data loss and destruction. Western sends full backups 30 miles to an annually contracted facility on a weekly basis.

c. Remote Operation

In conformance with SPR Design Criteria, the functional specification for the SPR DCS excluded the remote operability of the process equipment. FE operational and security concerns outweighed the potential benefits. The manual operation of the site's process equipment as backup to total DCS failure is significantly less costly than providing for remote operability.

The SAACS has a fail-over scheme to mitigate loss of functionality at either the Forrestal or the Germantown facility which are sites for system backups. Both facilities have host computers that are capable of performing all system functions or operating in a standalone configuration, with restoration based on the assumption that the system host computers and peripherals are available and in operating condition.

Western agrees an offsite control center for remote system operation will increase Western's ability to maintain control of its substation and transmission facilities in the event of a catastrophic event at the Folsom Office. There is a high availability system at the regional office facility and Western has taken appropriate actions to implement the offsite control center in 2005.

EM disagrees with the recommendation to implement a remote control capability for the Defense Waste Processing Facility (DWPF) Distributed Control System emergency operations as EM believes it is ill-advised and not common practice in the nuclear operations field. The DWPF was designed to operate without a remote capability. NIST 800-30, *Risk Management Guide for Information Technology Systems*, requires risk to be deliberated and formalized through documentation, which Savannah River has performed and completed in due diligence. The DWPF has a backup system as a contingency measure.

**Recommendation 2**

All of the Program Offices have plans to implement a comprehensive risk management process for their critical monitoring and control systems and will periodically evaluate

and strengthen management controls over these systems. The Program Offices will also continue to elicit peer reviews of all critical systems and engage Departmental expertise where appropriate.

If you have any questions or comments, please contact Stan Wujcik, Acting Director of Engineering and Assessments, at (301) 903-3434.

IG Report No. OAS-M-05-06

# CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost
effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form