**OFFICE OF**
**THE INSPECTOR GENERAL**

U.S. NUCLEAR
REGULATORY COMMISSION

NRC'S EFFORTS TO PROTECT
ITS CRITICAL INFRASTRUCTURE:
PRESIDENTIAL DECISION
DIRECTIVE 63

OIG-00-A-02 September 29, 2000

# AUDIT REPORT

September 29, 2000

MEMORANDUM TO: William D. Travers
Executive Director for Operations

Stuart Reiter
Acting Chief Information Officer

FROM: Stephen D. Dingbaum ***/RA/***
Assistant Inspector General for Audits

SUBJECT: REVIEW OF NRC'S EFFORTS TO PROTECT ITS CRITICAL INFRASTRUCTURE: PRESIDENTIAL DECISION DIRECTIVE 63

Attached is the Office of the Inspector General's audit report titled, *NRC's Efforts to Protect its Critical Infrastructure: Presidential Decision Directive 63* (PDD 63). The report incorporates comments provided by your offices, as appropriate, within the body of the report and includes them in their entirety in Appendix IV.

PDD 63 requires NRC and other agencies to develop a plan to eliminate any significant vulnerability to both physical and cyber attacks on their critical infrastructures. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. While NRC has made good progress toward meeting the goals of PDD 63, the Agency will need to more carefully examine the full scope of the Directive's requirements to complete its planning and assessment efforts. Additional senior management support will also help to ensure that the Agency's effort to protect the nation's critical infrastructure is efficiently and effectively planned and implemented. This report makes four recommendations to improve the Agency's efforts.

In accordance with the attached resolution procedures, please provide your response to the report and information on actions taken or planned on each of the recommendations directed to your office within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow up and reporting in accordance with the agreed upon resolution procedures.

If you have any questions, please call me at 415-5915.

Attachment: As Stated

cc: R. McOsker, OCM/RAM
B. Torres, ACMUI
B. Garrick, ACNW
D. Powers, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, GC
J. Cordes, Acting OCAA
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
F. Miraglia, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
J. Craig, AO/OEDO
M. Springer, ADM
R. Borchardt, OE
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
W. Kane, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, OSP
F. Congel, IRO
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

# EXECUTIVE SUMMARY

## Purpose

In May 1998, President Clinton issued *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (PDD 63) to initiate a national effort to ensure the security of the nation's critical infrastructures. Because of the importance of this effort, the Office of the Inspector General initiated a review of the Nuclear Regulatory Commission's (NRC) efforts to meet the requirements of the Directive. Our review was conducted in conjunction with a national review being performed under the President's Council on Integrity and Efficiency, and the Executive Council on Integrity and Efficiency. This report reflects the results of the first phase of the review, addressing planning and assessment for cyber-based infrastructures.

## Background

PDD 63 requires NRC and other agencies to develop a plan to eliminate any significant vulnerability to both physical and cyber attacks on their critical infrastructures. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government.

## Results in Brief

While NRC has made good progress toward meeting the goals of PDD 63, the Agency will need to more carefully examine the full scope of the Directive's requirements to complete its planning and assessment efforts. Additional senior management support will also help to ensure that the Agency's effort to protect the nation's critical infrastructure is efficiently and effectively planned and implemented.

## Recommendations

This report makes four recommendations to improve the Agency's efforts.

# TABLE OF CONTENTS

# INTRODUCTION

In May 1998, President Clinton issued *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (PDD 63) to initiate a national effort to ensure the security of the nation's critical infrastructures.[1] This Directive requires the Nuclear Regulatory Commission (NRC) and other agencies to develop a plan to eliminate any significant vulnerability to both physical and cyber attacks on their critical infrastructures. Because of the importance of this effort, the Office of the Inspector General initiated a review of NRC's efforts to meet the requirements of the Directive.

In addition, in late 1999, the President's Council on Integrity and Efficiency (PCIE)[2] and the Executive Council on Integrity and Efficiency (ECIE)[3] initiated a national effort to review the adequacy of the overall Federal Government effort. PCIE and ECIE proposed that the review be completed in four phases. The first phase, addressing planning and assessment for cyber-based infrastructures, began in January 2000. This review was conducted in conjunction with the PCIE/ECIE national effort. Appendix I contains information about our objectives, scope, and methodology.

## BACKGROUND

The Clinton Administration's policy calls for a national effort to ensure the security of the nation's critical infrastructures - also known as mission essential infrastructure. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and other essential government services. NRC, in the national picture, falls under the energy sector for PDD 63, but, as a Phase II agency, has no sector responsibility itself. NRC supports the Department of Energy (DOE) which has lead responsibility in the energy sector.

---

1 The national Critical Infrastructure Assurance Office has defined agency critical infrastructure or mission-essential infrastructure as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services." The Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, as amended, established NRC's regulatory mission to: (1) regulate the Nation's civilian use of byproduct, source, and special nuclear materials (2) ensure adequate protection of the public health and safety, (3) promote the common defense and security, and (4) to protect the environment.

2 Established by executive order, PCIE is comprised of all Presidentially appointed Inspectors General. PCIE is charged with conducting interagency and inter-entity audit, inspection and investigation projects to effectively and efficiently deal with government-wide issues of fraud, waste and abuse.

3 The ECIE is comprised mainly of the designated Inspectors General. An ECIE member serves as a Council representative on each of the PCIE Committees.

Of recent concern are advances in information technology that have caused many infrastructures to become increasingly automated and inter-linked, and have created new vulnerabilities to equipment failures, human error, weather, and physical and cyber attacks.[4] Attacks on both physical and cyber infrastructure may be capable of significantly harming our economic and military power.

The President intends that the United States take all necessary measures to eliminate significant vulnerabilities to both physical and cyber attacks on our nation's critical infrastructures focusing especially on cyber-systems. By May 22, 2003, the United States is expected to have achieved and should be able to maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

PDD 63 designates 12 "Phase I" lead agencies with major sector or Federal government-specific responsibilities. Phase I agencies are to encourage and support their counterparts in industry and state and local governments to develop and incorporate their own plans into the National Infrastructure Assurance Plan. This Plan includes awareness, vulnerability assessment, and information sharing initiatives. In addition, lead agencies have been designated for functions that must be chiefly performed by the Federal government (national defense, foreign affairs, intelligence, law enforcement, and research and development). Other agencies subject to PDD 63 are responsible for protecting their own assets but are not "lead agencies" for external national sectors. The eight agencies comprising the latter group are called Phase II agencies and include NRC. Appendix II provides a listing of Phase I and II agencies. Under PDD 63, the Chief Information Officer of each Phase I and Phase II agency is responsible for information assurance and a Chief Infrastructure Assurance Officer (CIAO) is responsible for the protection of all of the other aspects of the agency's critical infrastructure. NRC appointed the Director of the Incident Response Operations office as its CIAO.

---

4 As used here, cyber attacks, or cyber terror, may be defined as the unauthorized electronic access, manipulation or destruction of electronic data or code that is being processed, stored or transmitted on electronic media, having the effect of actual or potential harm to the nation's critical infrastructure.

For each agency involved, a major component of PDD 63 requirements is the development and implementation of a critical infrastructure protection plan (CIPP). NRC submitted the first version of its CIPP[5] to the national Critical Infrastructure Assurance Office in February 1999 and a revised version, based on comments from an external Expert Review Team, in May 1999.

## RESULTS OF REVIEW

While NRC has made good progress in its effort to meet PDD 63 requirements for the protection of its critical infrastructure, additional senior management attention is needed. This support will help to ensure that the Agency's effort to protect its own critical infrastructure and to support DOE efforts in the energy sector is successful. Because NRC's review started with Year 2000 (Y2K) work, the Agency has not conducted a review sufficiently comprehensive to fully consider the range of potential critical infrastructure systems and assets which should be addressed in its CIPP. In addition, the Agency needs to define the responsibilities and authority of its CIAO.

### FURTHER EFFORT IS NEEDED TO COMPLETE CRITICAL INFRASTRUCTURE PLANNING

NRC began identifying its critical infrastructure by using the results of Y2K efforts. In performing Y2K work, NRC developed an inventory of systems that included a ranking based on the criticality of the system to Agency operations. Seven systems were identified as mission-critical or the highest risk systems. From those, NRC narrowed the number to a single system, located in the office of Incident Response Operations (IRO),[6] which it deemed to fit the criteria for critical infrastructure. However, the implications of critical infrastructure extend beyond the general scope of Y2K evaluation to potentially include systems containing classified information, systems that involve interdependencies with other entities, and systems that relate to activities connected with national security (see footnote [1] for the definition of critical infrastructure). However, NRC did not consider the potential for these other types of critical infrastructure issues in starting with its Y2K inventory. For example:

---

5 The Plan is fully titled *United States Nuclear Regulatory Commission (NRC) Critical Infrastructure Protection Plan in Response to Presidential Decision Directive 63 (PDD-63)*, Version 1.0, January 31, 1999.

6 IRO directs the NRC program for response to incidents, and is the agency incident response interface with the Federal Emergency Management Agency and other Federal agencies. IRO exercises oversight of the regional response programs, manages the NRC Operations Center, and receives, screens, and promptly recommunicates operational event information reported to the Operations Center.

- Executive Order 12656[7] requires NRC to: (1) recapture or authorize the recapture of special nuclear material (SNM)[8] from licensees where necessary to assure the use, preservation, or safeguarding of such materials for the common defense and security, as determined by the Commission or as requested by the Secretary of Energy, and (2) provide advice and technical assistance to Federal, State, and local officials and private sector organizations regarding radiation hazards and protective actions in national security emergencies. Information about SNM is maintained by DOE in a system located at Oak Ridge, Tennessee. NRC licensees submit information about their SNM holdings to this database. In addition, NRC may need access to information relating to the provision of advice and technical assistance to other entities as described above. However, the CIPP does not address these issues.

- The National Security Telecommunications and Information Systems Security Committee (NSTISSC)[9] states that national security systems include systems that process classified information. NRC maintains classified information on restricted-use laptops and on a few personal computers (these PCs are not connected to NRC's network but have secured external links). This information, and the systems and assets it resides on, are not addressed as critical infrastructure in the CIPP.

- Executive Order 12472[10] provides NRC (and all Federal departments and agencies) with responsibilities for national security and emergency preparedness telecommunications functions. These responsibilities must be carried out in conjunction with the Federal Emergency Management Agency (FEMA) and others. In addition, communication with FEMA is part of NRC's emergency response procedures related to licensee events. While communication with FEMA is discussed in the CIPP, it is not addressed in the CIPP as critical infrastructure.

---

7 Executive Order 12656 is titled *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988.

8 SNM is defined in 10 CFR 20.1003 as "(1) Plutonium, uranium-233, uranium enriched in the isotope 233 or in isotope 235, and any other material that the NRC, pursuant to the provisions of section 51 of the AEA [the Atomic Energy Act of 1954], determines to be SNM, but does not include source material; (2) or any material artificially enriched by any of the foregoing but does not include source material." SNM is important in the fabrication of weapons grade materials and as such has strict licensing and handling controls.

9 NSTISSC sets national policy and promulgates direction, operational procedures, and guidance for the security of national security systems. NSTISSC is composed of members from 21 U.S. Government executive branch departments and agencies as well as observers from 11 additional departments and agencies.

10 Executive Order 12472 is titled *Assignment of national security and emergency preparedness telecommunications functions*, dated April 3, 1984.

NRC's CIPP makes good progress in addressing the Agency's activities in preparing for PDD 63 requirements. However, the above examples indicate that the Agency needs to reexamine its approach to ensure that it includes all critical infrastructure systems and assets that should be addressed in its CIPP.

In addition, while staff submitted a paper to the Commission describing the implications of PDD 63 in a general sense, staff has not provided the Commission with NRC's own plan, the CIPP, for addressing the Directive's requirements. Staff did submit a paper to the Commission containing its plan to address a similar PDD.[11] This provided senior management attention crucial to that work. Similar attention is warranted in a significant national effort such as that under PDD 63 to ensure that the Directive is adequately addressed.

NRC's Office of the Chief Information Officer prepared the Agency's CIPP, which focuses on internal systems. However, NRC must also consider the implications of such efforts with regard to its licensees. To that end, Agency personnel met with DOE officials to discuss NRC's role in supporting DOE's work as the lead agency for the Energy Sector.

Stemming from its own initiative and from the discussions with DOE, NRC's Office of Nuclear Materials Safety and Safeguards began work on a second plan, separate from the CIPP, to cover PDD 63 requirements and other related activities with its licensees. As a result, the Agency has two separate efforts underway: (1) internal -- reflected in the CIPP, and (2) external -- titled *NRC Action Plan in Response to PDD 63*. At the time of our review, the NRC Action Plan was in draft and the Agency did not plan to integrate the Action Plan with the CIPP. To maintain a consistent approach to PDD 63 and to ensure the Directive is fully addressed, NRC should integrate those portions of the Action Plan related to PDD 63, at least by reference, into the CIPP.

Finally, PDD 63 states that the CIAO is responsible for the protection of all aspects of the Agency's critical infrastructure other than information assurance, a CIO responsibility. However, NRC has not yet formally defined the authority and responsibilities of its CIAO. To ensure that the CIAO can function effectively in ensuring the Agency carries out its responsibilities under the Directive, NRC should provide a formal definition of the CIAO's authority and responsibilities.

## CONCLUSIONS

While NRC has made good progress toward meeting the goals of PDD 63, the Agency still needs to more fully examine the scope of the Directive's requirements and incorporate PDD 63-related efforts in the Action Plan in the

11 Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 1998.

CIPP. Also, the support and concurrence of the Commission will help to ensure that the Agency's effort to protect the nation's critical infrastructure is efficiently and effectively planned and implemented. Finally, the Agency needs to formally establish the responsibilities and authority of the CIAO to ensure the effective functioning of that important position.

## RECOMMENDATIONS

To ensure that NRC fully addresses the requirements of PDD 63, we recommend that the Executive Director for Operations and the Chief Information Officer:

1. Identify all elements of NRC's critical infrastructure to ensure that the full scope of the Directive is addressed.

2. Incorporate the PDD 63-relevant portions of the Action Plan, at least by reference, into the CIPP.

3. Provide a time line for the Commission to receive and approve the CIPP.

We also recommend that the Executive Director for Operations:

4. Develop a formal description of the responsibilities and authority of the CIAO.

## OIG COMMENTS ON THE AGENCY'S RESPONSE

On September 21, 2000, the Executive Director for Operations and the Acting Chief Information Officer responded to our draft report and agreed with our recommendations. In addition, they provided editorial comments on the report. Based on those comments, we made changes to the report where appropriate. Their response is included as Appendix IV.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of our review was to assess the adequacy of the Nuclear Regulatory Commission's (NRC) efforts to address the requirements of Presidential Decision Directive 63. The overall review was proposed to consist of four phases. Phases I and II relate to critical cyber-based infrastructures and Phases III and IV relate to critical physical infrastructures. This report contains results for Phase I only. In Phase I we reviewed the adequacy of agency planning and assessment activities for protecting their critical, cyber-based infrastructures. Specifically, we reviewed the adequacy of agency plans, asset identification efforts, and initial vulnerability assessments. The objectives for Phase I of the audit were to:

1. Identify past and present issues related to NRC's critical infrastructure, and the criteria and management roles and responsibilities related to its program.

2. Determine whether NRC has developed an effective plan for protecting its critical cyber-based infrastructures.

3. Determine whether NRC has identified its cyber-based critical infrastructure and interdependencies.[12]

4. Determine whether NRC has adequately identified the threats, vulnerabilities, and potential magnitude of harm to its cyber-based critical infrastructure that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of its critical cyber-based infrastructure investments.

Our review was based on guidance developed by a President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency working group in conjunction with the many Offices of the Inspector General which are participating. To accomplish our objectives, we reviewed NRC's critical infrastructure protection plan and the planning and assessment that led to NRC's identification of critical infrastructure. We interviewed cognizant NRC officials in the Offices of the Chief Information Officer, Nuclear Materials Safety and Safeguards, and Incident Response Operations. We also met with officials from other Offices of the Inspector General. In addition, we reviewed related guidance and criteria developed by the national Critical Infrastructure Assurance Office, the General Accounting Office, and others.

We evaluated the management controls related to NRC's critical infrastructure program and conducted our audit from January 2000 through June 2000 in accordance with generally accepted Government auditing standards.

---

12 Interdependence is defined by the National Plan for Information Systems Protection as "Dependence among elements or sites of different infrastructures, and therefore, effects by one infrastructure upon another."

## PHASE I and PHASE II AGENCIES

| **Phase I Lead Agency** | **Critical Infrastructure Sector** |
|---|---|
| Commerce | Information and communications |
| Treasury | Banking and finance |
| Environmental Protection Agency | Water supply |
| Transportation | Aviation, Highways, Mass transit, Pipelines, Rail, Waterborne commerce |
| Justice/FBI | Emergency law enforcement services |
| Federal Emergency Management Agency | Emergency fire service, Continuity of government services |
| Health and Human Services | Public health services |
| Energy | Electric power, Oil and gas production and storage |
| Phase I Lead Agencies for Special Functions | Special Function Area |
| Justice/FBI | Law enforcement and internal security |
| Central Intelligence Agency | Foreign intelligence |
| State | Foreign affairs |
| Defense | National defense |
| Office of Science and Technology Policy | Research and development |
| **Phase II Agencies** (no sector responsibility) | |
| Agriculture | General Services Administration |
| Education | Labor |
| Housing and Urban Development | National Aeronautics and Space Administration |
| Interior | Nuclear Regulatory Commission |

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| CIAO | Chief Infrastructure Assurance Officer |
| CIPP | Critical Infrastructure Protection Plan |
| DOE | Department of Energy |
| ECIE | Executive Council on Integrity and Efficiency |
| FEMA | Federal Emergency Management Agency |
| IRO | Incident Response Operations |
| NRC | U.S. Nuclear Regulatory Commission |
| NSTISSC | National Security Telecommunications and Information Systems Security Committee |
| PCIE | President's Council on Integrity and Efficiency |
| PDD | Presidential Decision Directive |
| SNM | Special Nuclear Material |
| Y2K | Year 2000 |

## AGENCY RESPONSE TO DRAFT REPORT

**September 21, 2000**

MEMORANDUM TO: Stephen D. Dingbaum
Assistant Inspector General for Audits
Office of the Inspector General

FROM: William D. Travers **/RA Frank J. Miraglia Acting For/**
Executive Director for Operations

Stuart Reiter **/RA/**
Acting Chief Information Officer

SUBJECT: DRAFT AUDIT REPORT - NRC'S EFFORTS TO PROTECT INFORMATION TECHNOLOGY CRITICAL INFRASTRUCTURE: PRESIDENTIAL DECISION DIRECTIVE 63

This memorandum responds to your draft audit report dated September 15, 2000, regarding the NRC's efforts to protect its critical infrastructure pursuant to Presidential Decision Directive 63 (PDD-63). As discussed in the report and in PDD-63, there are 12 "Phase I" agencies, with sector or Federal government-specific responsibilities. NRC is a "Phase II" agency with no sector responsibility other than to support the sector lead (DOE).

Upon receiving the report, we convened a core group of staff to review the report and its recommendations on the PDD-63 initiative. This core group consisted of the staff involved in developing the NRC Critical Infrastructure Protection Plan (CIPP) as well as the staff who have been working to support DOE with their responsibility for the Energy sector under the PDD-63 initiative.

We appreciate the opportunity to have met with your staff to discuss this report after our initial review. Based on that meeting and our review of the revised draft report, the attached comments reflect factual clarification and editorial recommendations. With these clarifications, we agree with the report's conclusion and recommendations. We also note that the report acknowledges the progress that the staff has made to meet the goals of PDD-63.

In addition to our response, we see no reason that the report should not be publicly released.

If you have any further questions or concerns about this matter, please contact Debra Corley at 415-1728.

Attachment:
As stated

STAFF COMMENTS ON REVISED DRAFT OIG AUDIT REPORT ON
PRESIDENTIAL DECISION DIRECTIVE 63 (PDD-63)

1. Page 1, Recommendations section: change "three" recommendations to "four"

2. Page 4, Background section, 1st paragraph, last sentence ("NRC's role at the national level falls in the energy sector.):

   Recommend deleting this sentence (this paragraph and the following two paragraphs discuss critical infrastructure background. Agency roles and responsibilities, including NRC's, are discussed on page 5). If not deleted, propose revising as follows: "NRC falls under the Energy sector for PDD-63, but as a Phase II agency, has no sector responsibility.

3. Page 6, Results of Review section, 1st sentence:

   Delete the word "protect" and add the words "**support DOE in protecting**" ("....to help ensure that the Agency's efforts to ~~protect~~ support DOE in protecting the nation's critical infrastructure.....")

4. Page 6, Results of Review section, 2nd sentence:

   Recommend revising this sentence as follows: Although NRC's review ~~In particular, because it~~ started with Year 2000 (Y2K) work, it does not appear that the Agency ~~has not~~ completed a comprehensive review to fully consider~~ed~~ the range of potential critical infrastructure systems....."

5. Page 7, Further Effort is Needed to Complete Critical Infrastructure Planning section, last sentence:

   Recommend revising this sentence as follows: "However, it did not appear that NRC ~~did not~~ considered the potential for ....."

6. Page 9, 1st paragraph after bullet, 2nd sentence:

   Recommend revising this sentence as follows: "However, the above examples indicate that the Agency needs to ~~take a more comprehensive~~ reexamine its approach to ensure....."

7. Page 10, 1st full paragraph:

   Recommend deleting this paragraph ("NRC's Office of the Chief Information Officer prepared the Agency's CIPP....."). NRC, as a Phase II agency under PDD-63, has no Energy sector responsibility. NRC, on its own initiative, however, plans to provide support to DOE as the lead agency for the Energy sector.

8. Page 10, 2nd paragraph, 3rd sentence:

   Recommend revising this sentence as follows: "At the time of our review, the NRC Action Plan in Response to PDD-63 was a draft plan, and at that point in time the Agency did not plan to integrate the Action Plan with the CIPP."

9. Page 12, Recommendation 2:

   Recommend revising the recommendation to be consistent with the text in the report (page 10) as follows: "Incorporate the PDD-63 relevant portions of the Action Plan, at least by reference, into the CIPP.

**AUDITORS NOTE:** Pages identified in the staff comments referring to the draft report are now found in the final report as follows:

1. Page 1 remains Page 1.

2. Page 4 is now Page 3.

3. Page 6 is now Page 5.

4. Page 6 is now Page 5.

5. Page 7 is now Page 5.

6. Page 9 is now Page 7, 1st paragraph, 2nd sentence.

7. Page 10 is now Page 7, 3rd paragraph.

8. Page 10 is now Page 7, 4th paragraph, 3rd sentence.

9. Page 12 is now Page 8.

## MAJOR CONTRIBUTORS TO THIS REPORT

William McDowell
Team Leader

Robert Moody
Audit Manager