

EDO Principal Correspondence Control

FROM: DUE: 02/11/09

EDO CONTROL: G20090055
DOC DT: 02/03/09
FINAL REPLY:

James T. MacAulay, GAO

TO:

Arildsen, OEDO

FOR SIGNATURE OF :

** GRN **

CRC NO:

Arildsen, OEDO

DESC:

ROUTING:

Federal Cyber Critical Infrastructure Planning
- GAO Job Code: 310877 (NOT IN EDATS)

Borchardt
Virgilio
Mallett
Ash
Ordaz
Cyr/Burns
Hagan, ADM
Howard, CSO
Cyr, OGC
GAO File

DATE: 02/04/09

ASSIGNED TO:

CONTACT:

EDO
NSIR

Arildsen
Zimmerman

SPECIAL INSTRUCTIONS OR REMARKS:

NSIR to take lead in coordination with ADM, CSO and OGC to provide response for OEDO to forward to GAO.

Attached are two documents the NRC submitted to GAO (referenced in the request). Provide input to Jesse Arildsen by February 10, 2009. Jesse to respond to GAO by February 11, 2009.

Cathy Jaegers

From: James T. MacAulay [MacAulayJ@gao.gov]
Sent: Tuesday, February 03, 2009 11:50 AM
To: Jesse Arildsen
Cc: Kenneth A Johnson
Subject: Follow-up: Job Code 310877

Dear Mr. Arildsen,

We are wrapping up the analysis phase of our review of Federal Cyber Critical Infrastructure Planning, job code 310877. At the time of OMB's 2004 reporting requirement, your agency indicated that it did not have any cyber critical infrastructure assets to report, as defined by HSPD-7. However, we wanted to follow-up to make sure that statement is still an accurate portrayal of your agency. Further, we would like to obtain any updated information or plans that would have an impact on the status of your 2004 submission to OMB. If there have been no changes please indicate that in your response to this message.

We would greatly appreciate if you could respond to this request no later than the COB of 02/11/09. Please feel free to contact me if you have any questions or would like to discuss further.

Sincerely,

Jim

James T. MacAulay
IT Analyst
U.S. Government Accountability Office
441 G Street, NW, Mail Room 4T21
Washington, D.C. 20548

Phone: (202)-512-2775
Email: MacAulayJ@gao.gov

Received: from mail2.nrc.gov (148.184.176.43) by OWMS01.nrc.gov
(148.184.100.43) with Microsoft SMTP Server id 8.1.291.1; Tue, 3 Feb 2009
11:49:53 -0500

X-Ironport-ID: mail2

X-SBRS: 4.5

X-MID: 25354383

X-IronPort-Anti-Spam-Filtered: true

X-IronPort-Anti-Spam-Result:

AgcCAMMEiEmhyxAVkWdsb2JhbACUJgEBAQEJCwoHEQWsrAmOQQGCYIEzBg

X-IronPort-AV: E=Sophos;i="4.37,373,1231131600";

d="scan'208";a="25354383"

Received: from mxout.gao.gov ([161.203.16.21]) by mail2.nrc.gov with ESMTP;
03 Feb 2009 11:49:53 -0500

Received: from GAOTVCS1 (mxin.gao.gov [161.203.16.22]) by mxout.gao.gov
(8.13.6/8.13.6) with ESMTP id n13GnqqO014795 for <Jesse.Arildsen@nrc.gov>;
Tue, 3 Feb 2009 11:49:52 -0500

Received: from GAOMAIL2.GAO.GOV ([161.203.15.24]unverified) by mxin.gao.gov
with InterScan Message Security Suite; Tue, 03 Feb 2009 11:49:48 -0500

Received: from GWIADOM-MTA by GAOMAIL2.GAO.GOVwith Novell_GroupWise; Tue, 03
Feb 2009 11:49:47 -0500

Message-ID: <49882121.ED17.0079.0@GAO.GOV>

X-Mailer: Novell GroupWise Internet Agent 7.0.3

Date: Tue, 3 Feb 2009 11:49:44 -0500

From: "James T. MacAulay" <MacAulayJ@gao.gov>

To: <Jesse.Arildsen@nrc.gov>

CC: "Kenneth A Johnson" <Johnsonk@GAO.GOV>

Subject: Follow-up: Job Code 310877

MIME-Version: 1.0

Content-Type: text/plain; charset="US-ASCII"

Content-Transfer-Encoding: quoted-printable

Content-Disposition: inline

Return-Path: MacAulayJ@gao.gov

Critical Infrastructure Protection Plan (CIPP)

U.S. Nuclear Regulatory Commission

Office of Nuclear Security and Incident Response

July 2004, Rev. 3

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552)

Exemption Number 2
Nuclear Regulatory Commission review required before public release.

Eric M. Thomas, NSIR/IRD
Name and organization of person making determination.

Date of Determination July 12, 2004

FOREWORD

In December 2003, the President issued Homeland Security Presidential Directive (HSPD) 7, which directs all Federal departments and agencies to develop and submit plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans are designated Critical Infrastructure Protection Plans (CIPPs). The U.S. Nuclear Regulatory Commission (NRC) previously submitted CIPPs in 1999 and 2001 in response to Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," which was issued in May 1998.

In preparing this revision of the plan, the NRC responded to additional guidance from the Office of Management and Budget (OMB) including answers to specific questions that are contained in an addendum to the updated CIPP.

1. BACKGROUND

1.1 Introduction

In December 2003, the President issued Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization and Protection," which "establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." Critical infrastructure is defined in Section 1016 of the Patriot Act of 2001 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Key resources are defined in the Homeland Security Act of 2002 as "publicly or privately controlled resources essential to the minimal operations of the economy and government."

Paragraph 34 of HSPD-7 directs all Federal departments and agencies to develop and submit plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans are designated Critical Infrastructure Protection Plans (CIPPs). The NRC previously submitted CIPPs in 1999 and 2001 to the Critical Infrastructure Assurance Office in response to Presidential Decision Directive (PDD) 63, "Critical Infrastructure Protection," which was issued in May 1998. Per HSPD-7, the CIPP "shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities."

1.2 Other Initiatives

Paragraph 29 of HSPD-7 directs the Department of Homeland Security (DHS) to work with the U.S. Nuclear Regulatory Commission (NRC) and the Department of Energy (DOE) to ensure the necessary protection of commercial power and non-power nuclear reactors; certain nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste. Planned protection activities for this sector are described in the National Infrastructure Protection Plan (NIPP), Sector Specific Plan (SSP) for Commercial Nuclear Reactors, Materials, Waste, and Storage. The initial draft of the NIPP was submitted to DHS in June 2004, and updated in July 2004.

PDD 67, "Enduring Constitutional Government and Continuity of Government Operations," was issued in October 1998, and required agencies to develop Continuity of Operations Plans (COOPs) to ensure that they could continue to perform their essential functions under severe adverse conditions. PDD 67 incorporated the general requirements of PDD 63, but shifted the focus of these requirements from protecting *systems* to protecting *functions*. This shift was reflected in the 2001 NRC CIPP, which stated that the agency had no critical infrastructure. The COOP provides a documented procedure by which the essential functions of NRC Headquarters can be shifted to an alternate site. The 2001 CIPP updated the 1999 CIPP to reflect the fact that the NRC does not have any critical infrastructure as defined in PDD 63.

1.3 Purpose, Scope, and Format

This plan replaces the CIPP submitted by the NRC in 1999 and in 2001 in response to the requirements of PDD 63 and fulfills the new requirements of HSPD-7, the Homeland

OFFICIAL USE ONLY

Security Act, the Patriot Act and the guidance provided by the Office of Management and Budget (OMB). In this Plan, the NRC staff uses definitions from the Patriot and Homeland Security Acts, along with past reports and letters, to justify the determination that, as stated in the 2001 CIPP and elsewhere, that NRC does not have any critical infrastructure or key resources.

The format for the CIPP was provided by OMB. It instructs each department to:

- describe existing processes and approaches for protecting Federal critical infrastructure and key resources
- provide future plans for protecting critical infrastructure/key resources

The Staff conducted a review of NRC assets to the criteria specified in HSPD-7 and determined that none of the agency's systems or components are designated as critical infrastructure or key resources. Therefore, this revision to the CIPP need not provide discrete answers to many of the OMB questions. However, the Plan does describe how the NRC protects its ability to perform certain minimal essential functions.

2. RESPONSIBILITIES

2.1 Chief Information Officer (CIO)

The CIO plans, directs, and oversees the delivery of centralized information technology applications and information management services to the NRC. The CIO is responsible for information assurance. Among the specific CIO responsibilities related to this CIPP is the following:

- Direct NRC's computer and information security program, including training of NRC personnel with respect to information systems that are critical to NRC's business functions, but are not "critical infrastructure" as defined in the Patriot Act.

2.2 Chief Infrastructure Assurance Officer (CIAO), Office of Nuclear Security and Incident Response

The CIAO is responsible for coordinating all NRC critical infrastructure protection activities that are not the direct responsibility of the CIO. Those activities include the following:

- Ensure that OCIO provides adequate training to NRC personnel to sensitize them to the security aspects of protecting the agency's critical business functions
- Ensure that CIPP-related systems are properly certified by the CIO in accordance with A-130 and NRC Management Directive 12.5 or future requirements
- Represent the NRC to the Office of Management and Budget and approve all formal correspondence to that office

OFFICIAL USE ONLY

- Review and approve the CIPP and all proposed changes thereto
- Coordinate NRC support for the Department of Energy (DOE), which is the lead agency for HSPD-7 efforts in the national energy sector (other than commercial power reactors)
- Maintain the all-hours NRC Operations Center (NRCOC) to receive threats and other emergency calls and to disseminate warnings as appropriate to NRC licensed activities
- Train agency personnel on the NRC's Continuity of Operations Plan, and update the plan as necessary
- Interface with other NRC offices and other Federal agencies concerning warnings and incidents affecting critical infrastructure and licensed reactor facilities and materials

The Director, Directorate of Incident Response Operations, Office of Nuclear Security and Incident Response, is the designated CIAO for NRC.

2.3 Director, Division of Facilities and Security (DFS), Office of Administration

DFS (1) establishes policy and (2) plans and directs the agency's real property and building management programs. CIPP-related DFS functions include the following:

- Plan, develop, establish, and administer policies and procedures for the overall program for NRC physical security, including the protection of classified and sensitive unclassified systems that are determined to be critical to NRC's business functions
- Direct the physical protection of NRC Headquarters, regional offices, and other facilities that contain cyber systems that are determined to be critical to NRC's business functions

DFS works with OCIO on the development and implementation of physical security policies and plans as well as on joint assessments related to the agency's critical business functions.

3. ASSET IDENTIFICATION

3.1 Criteria for Identification of Critical Infrastructure

HSPD-7 instructs agencies to develop plans for protecting their physical and cyber critical infrastructure and key resources. These plans are to address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities. Critical infrastructure and key resources are defined in the Patriot Act and Homeland Security Act as follows:

OFFICIAL USE ONLY

- **Critical Infrastructure** - systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters
- **Key Resources** - publicly or privately controlled resources essential to the minimal operations of the economy and government

PDD 67 requires agencies to identify their minimum essential *functions*, rather than *systems*. Minimum essential functions are those that are so important to the agency that they must be restored within 12 hours after a severe interruption and must be maintained for up to 30 days at alternate locations, if necessary. The NRC uses the term "mission-critical" to define all non redundant information technology systems needed to support the minimum essential functions of the agency.

3.2 NRC Critical Infrastructure Under HSPD-7

This section reviews current NRC assets against the criteria of Section 3.1 and the requirements of Section 1.1 to identify assets that require special protection in accordance with HSPD-7. The facilities, structures, and systems owned and operated by the NRC are not categorized as critical infrastructure or key resources. Therefore, under paragraph 34 of HSPD-7, the NRC has *no* critical infrastructure or key resources as defined in the Patriot Act and Homeland Security Act.

Paragraph 34 of HSPD-7 also mentions that the CIPP shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities. The NRC's recovery and reconstitution of essential capabilities can be categorized as an essential *function* that must be protected under PDD 67. The NRC's mission is to regulate the nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. In this undertaking, the NRC oversees nuclear power plants; research, test, and training reactors; nuclear fuel cycle facilities; the industrial, academic, and medical uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste. NRC works closely with its licensees and with local, State, other Federal, and international organizations so that the agency can achieve its goals in the event of an emergency. The agency's essential capabilities in the sense of HSPD-7 (minimum essential functions in PDD 67) are defined in the NRC COOP Plan as:

- functions necessary to minimize immediate threats to public health and safety by responding to problems involving regulated activities
- emergency decision making functions (i.e., functions necessary to enable appropriate NRC authorities to make and communicate decisions about problems involving regulated activities, to interact with NRC staff, and to interact with other authorities as necessary to implement the COOP Plan)

These are the only NRC functions that can have an immediate effect on the health and safety of the public. In accordance with Section 3.1, NRC systems needed to support

OFFICIAL USE ONLY

these functions would be considered mission-critical if they were not otherwise protected.

However, the agency's minimum essential functions are protected by provisions of the COOP Plan, as PDD 67 requires. If, for any reason, Headquarters can no longer perform its emergency response functions, the responsibility for those functions shifts to an alternate NRC site under the COOP Plan. A telephone call from any location to one of the telephone company's special centers can redirect all emergency telephone lines from the NRCOC to the alternate COOP site, from which response personnel can establish telephone conferences with other qualified NRC response personnel and decisionmakers as needed, wherever they may be. As a result, nothing within the Headquarters complex, including the NRCOC itself, is needed to maintain minimum essential functions and nothing is designated mission-critical at this time.

4. PLAN MAINTENANCE

4.1 Tasks

HSPD-7 requires an annual review of this CIPP. The review is essentially a determination of whether the NRC has added critical physical or cyber-based systems within the scope of HSPD-7. PDD 67 also requires an annual review of the NRC COOP Plan. Because the two plans are intimately related, and the NRC has previously reviewed the CIPP annually with the COOP Plan, the agency will continue to do so. This joint review reflects the integrated status of minimum essential functions and supporting systems. The NRC has no critical infrastructure, so no additional CIPP updates are required unless and until a review determines that an agency asset meets the definition of critical infrastructure. If such a determination is made, the CIPP will be revised, and measures for asset protection will be established.

4.2 Schedule

CRITICAL INFRASTRUCTURE PROTECTION PLAN (CIPP)

Action	Schedule	Next Due
Review	This CIPP will be reviewed annually with the NRC COOP Plan	8 / 2005
Revise	If and when a system or function change causes some system to become mission-critical	When review shows need

**ADDENDUM: . NRC ANSWERS IN RESPONSE TO OMB CRITICAL
INFRASTRUCTURE PROTECTION PLAN GUIDANCE**

**Part 1: Describe existing processes and approaches for protecting Federal critical
infrastructure and key resources**

1. Background and Introduction

• **Summary of the primary business functions and activities of the NRC**

The Nuclear Regulatory Commission's (NRC's) mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. The NRC regulates in three main areas: nuclear reactors, nuclear materials, and nuclear waste. The nuclear reactor area covers commercial reactors for generating electric power and research and test reactors used for research, testing, and training. The nuclear materials area covers uses of nuclear materials in medical, industrial, and academic settings and facilities that produce nuclear fuel. The nuclear waste area covers transportation, storage, and disposal of nuclear materials and waste, and decommissioning of nuclear facilities from service.

The NRC's regulatory process has five main components: (1) developing orders, regulations and guidance for NRC applicants and licensees, (2) licensing or certifying applicants to use nuclear materials or operate nuclear facilities, (3) overseeing licensee operations and facilities to ensure that licensees comply with safety requirements, (4) evaluating operational experience at licensed facilities or involving licensed activities, and (5) conducting research, holding hearings to address the concerns of parties affected by agency decisions, and obtaining independent reviews to support NRC regulatory decisions.

• **Summary of the management structure of the NRC, including responsibilities for internal critical infrastructure/key resource protection, information security, physical security, personnel security, and continuity of operations programs.**

The NRC is headed by a five-member Commission. The President designates one Commissioner to serve as Chairman and official spokesperson. The Commission as a whole formulates policies and regulations governing the nuclear reactor, materials, and waste programs, issues orders to licensees, and adjudicates legal matters brought before it. The Executive Director for Operations (EDO) carries out the policies and decisions of the Commission and directs the activities of the program offices. The main NRC program offices are briefly described below.

The Office of Nuclear Reactor Regulation (NRR) is responsible for ensuring the public health and safety through licensing and inspection activities at all nuclear power reactor facilities in the United States. NRR is responsible for the oversight of all aspects of licensing and inspection of production and utilization facilities (except for facilities

OFFICIAL USE ONLY

reprocessing fuel and enrichment), and receipt, possession, and ownership of source, byproduct, and special nuclear material used or produced at facilities licensed under Part 50 of Title 10 of the Code of Federal Regulations.

The Office of Nuclear Materials Safety and Safeguards (NMSS) is responsible for ensuring the public health and safety through licensing, inspection, and environmental reviews for all activities regulated by the NRC, except operating power and all non-power reactors.

The Office of Nuclear Regulatory Research (RES) plans, recommends, and implements programs of nuclear regulatory research. RES also independently proposes improvements to the agency's regulatory programs and processes to achieve enhanced safety, efficiency, or effectiveness based on the results of this research.

The Office of Nuclear Security and Incident Response (NSIR) develops overall agency policy on security, emergency preparedness, and incident response; provides management direction for evaluation and assessment of technical issues involving security, preparedness, and response for nuclear facilities and materials; and is the agency interface with the Department of Homeland Security (DHS), the intelligence and law enforcement communities, and other agencies on security, preparedness, and response. NSIR is responsible for the NRC's Continuity of Operations (COOP) Plan.

The NRC has regional offices in King of Prussia, PA; Atlanta, GA; Lisle, IL; and Arlington, TX. The regional offices report to the EDO, and are responsible for executing established NRC policies and assigned programs relating to inspection, licensing, incident response, governmental liaison, resource management, and human resources.

The Office of the Chief Information Officer (CIO) plans, directs, and oversees the delivery of centralized information technology (IT) infrastructure, applications, and information management (IM) services, computer security, and the development and implementation of IT and IM plans, architecture, and policies to support the mission, goals, and priorities of the agency. The CIO represents the NRC on the Federal CIO Council, and advances the achievement of NRC's mission by assisting management in recognizing where IT can add value by transforming or supporting agency operations.

The Office of Administration (ADM), Division of Facilities Security is responsible for planning, developing, and administering policies and procedures for the overall program for NRC physical security and personnel security. Included are responsibilities for (1) physically protecting NRC facilities; (2) ensuring the safeguarding of classified and sensitive unclassified information at NRC and NRC contractor facilities; (3) managing the personnel security program; and (4) administering NRC's drug testing program.

- **Summary of the locations and assets (including contractor assets) that support the primary business functions and activities of the NRC.**

The NRC has its Headquarters in Rockville, Maryland and a number of other offices around the United States.

The two-building headquarters complex in Rockville, Maryland, houses the Headquarters staff, the Public Document Room, and the Headquarters Operations Center.

OFFICIAL USE ONLY

The Region I Office in King of Prussia, Pennsylvania, oversees the regulatory activities in the northeastern United States and material licensees in the southeastern United States.

The Region II Office in Atlanta, Georgia, oversees the regulatory power reactor activities in the southeastern United States and fuel cycle activities throughout the Nation.

The Region III Office in Lisle, Illinois, oversees the regulatory activities in the northern midwestern United States.

The Region IV Office in Arlington, Texas, oversees the regulatory activities in the western and southern mid western United States.

The On-Site Representative High-Level Waste Management Office in Las Vegas, Nevada, maintains an onsite presence at the proposed high-level waste repository.

The NRC Technical Training Center in Chattanooga, Tennessee, provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities.

In addition, the NRC maintains a local presence at all commercial nuclear power plants and major fuel cycle facilities through its resident inspector program. Resident inspectors occupy small offices at licensee facilities around the country.

2. Identify current capabilities for protecting internal critical infrastructure and key resources, covering the following activities:

- **Ability to identify Federally owned or operated (to include leased) critical infrastructure/key resource assets**

After considering the definitions set forth in the Homeland Security Act and the Patriot Act, the NRC has determined that it does not have any critical infrastructure or key resources. This is because none of the NRC's physical or virtual systems and assets are so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, or national public health and safety. In addition, none of the NRC's resources are essential to the minimum operations of the economy and government.

- **Ability to assess the vulnerabilities and interdependencies among assets**

The NRC defined its critical systems [i.e., assets] as those necessary to perform the agency's minimum essential functions:

- functions necessary to minimize immediate threats to public health and safety by responding to problems involving regulated activities
- emergency decisionmaking functions (i.e., functions necessary to enable appropriate NRC authorities to make and communicate decisions about problems involving regulated activities, to interact with NRC staff, and to interact with other authorities as necessary to implement the COOP Plan)

OFFICIAL USE ONLY

In general, these functions are carried out using the personnel, cyber, and security systems provided by the NRC Operations Center (NRCOC) and designated alternate COOP site. The NRCOC is staffed 24 hours each day with at least two qualified watchstanders on duty to respond to any problems reported by licensees or members of the public. The NRCOC staff accomplishes its duties using several relational databases and a robust telecommunications and teleconferencing system. The NRCOC can be quickly staffed with senior decisionmakers and technical experts at the NRC.

Any one of a number of deliberate attacks, unlikely events, or natural disasters could result in a complete loss of systems and personnel that normally perform the incident response functions of the NRCOC. Table 1, published as part of the NRC COOP, contains a comprehensive list of potential disruptions to normal NRC operations that could result in a transfer of normal NRCOC functions to the NRC's alternate COOP site.

- **Ability to prioritize among Federal assets based on vulnerability, consequence, and threat information**

None of the NRC's Federal assets cross the threshold to qualify as critical infrastructure or key resources.

- **Overall capability to adequately protect against threats to Federal critical infrastructure and key resource assets**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

- **Overall capability to respond to, and recover from, events that impair the ability to perform mission critical functions at or using Federal critical infrastructure or key resource assets**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act. However, the NRC COOP Plan does outline the procedures that the agency would follow to respond to and recover from events that impair its mission critical functions. If, for any reason, Headquarters can no longer perform its emergency response functions, the responsibility for those functions shifts to an alternate NRC site under the COOP Plan. A telephone call from any location to one of the telephone company's special centers can redirect all emergency telephone lines from the NRCOC to the alternate COOP site, from which response personnel can establish telephone conferences with other qualified NRC response personnel and decisionmakers as needed, wherever they may be.

OFFICIAL USE ONLY

TABLE 1. EXAMPLES OF POTENTIAL DISRUPTIONS TO NORMAL OPERATIONS

<p>To NRC operations</p> <p>1.a Evacuation of any regional office for natural or accidental causes; more disruptions unlikely</p> <p>1.b Evacuation of any regional office for deliberate causes, including sheltering in place in response to riots, attacks, and orders to seal the building; follow-on possible, duration uncertain</p> <p>2.a Evacuation of the NRC Operations Center (NRCOC) or Two White Flint North (TWFN) for natural or accidental causes; more disruptions unlikely</p> <p>2.b Evacuation of One White Flint North (OWFN) for natural or accidental causes; more disruptions unlikely</p> <p>2.c Evacuation of both OWFN and TWFN for natural or accidental causes; more disruptions unlikely</p> <p>3.a Evacuation of NRCOC, TWFN, or both OWFN and TWFN for security causes, but briefly because cause was non-terrorist-related or the perpetrator was caught; more disruptions unlikely</p> <p>3.b Evacuation of OWFN and TWFN for security causes, including sheltering in place in response to riots, attacks, and orders to seal the building; may be more disruptions, duration uncertain</p> <p>4.a Serious cyber attack that prevents effective use of the NRCOC and OWFN</p> <p>4.b Serious cyber attack that prevents effective use of any regional office</p>
<p>To the Washington area</p> <p>5.a Extended natural disaster, but NRCOC can function and response team can staff the NRCOC</p> <p>5.b Extended natural disaster; Operations Officers and HQ response team cannot function in the NRCOC</p> <p>6. Limited attack by weapons of mass destruction, actual or imminent, with some Federal evacuations that may or may not directly affect NRC</p>
<p>To licensee operations</p> <p>7. Confirmed cyber or physical attack at one or more facilities; more disruptions uncertain</p> <p>8. Unconfirmed cyber attack at one or more facilities; more disruptions uncertain</p>
<p>To national interests</p> <p>9.a Infrastructure loss (e.g., Internet, telecommunications, energy distribution) known to be non-terrorist-related or the perpetrator was caught; more disruptions unlikely</p> <p>9.b Unsolved infrastructure attack; more attacks possible</p> <p>10. Assaults against key individuals, concentrations of people, commercial infrastructure</p> <p>11. U.S. initiates military actions anywhere</p>

OFFICIAL USE ONLY

3. **Please identify the process for determining budget and personnel requirements for critical infrastructure and key resources protection, response, and reconstitution activities. Does the agency's FY04 appropriation and FY05 budget request include specific programs to protect the agency's critical infrastructure?**

While the NRC does not have any critical infrastructure or key resources as defined by the Homeland Security Act and the Patriot Act, there are budget and personnel requirements for response and reconstitution activities as they relate to NRC's minimum essential functions. These activities are carried out at the NRCOC and, as required by the NRC COOP, at the NRC's alternate site. The NRC's method of replicating critical *functions* rather than critical *assets* makes it difficult to assign particular dollar amounts to its expenditures in this area because the capabilities, personnel, and equipment utilized in response and reconstitution activities are not always neatly broken out into budgetary line items.

Table 2 lists the NRC's Incident Response Operations Planned Activities, along with the 2004 enacted, and 2005 requested FTE (full-time equivalent) and dollar amount expenditures associated with critical functions.

Table 2: Budget and Personnel Requirements

Headquarters Operations Center				
Activity	FY2004		FY2005	
	FTE	Enacted (\$K)	FTE	Requested (\$K)
NRCOC lighting system	0	7		7
Operations Center Information Management System (OCIMS)	1.5	2,490	1.5	814
Emergency Response Date System (ERDS)	0.5	504	0.5	1,800
Direct Access Line (DAL) service	0	0	0	100
Satellite phones	0	0	0	19
National Warning System	0	0	0	3
Redirect service	0	0	0	4
NRC Alternate Site				
Activity	FY2004		FY2005	
	FTE	Enacted (\$K)	FTE	Requested (\$K)
Backup Internet/Internet e-mail connection	0	30	0	30
Hardware, software, and LAN administration staff required to support and maintain the backup email capability, routing capability, firewall capability, intrusion detection capability, and antivirus capability	0	150	0	150

OFFICIAL USE ONLY

4. **Describe the process for ensuring independent oversight of CIP programs. Discuss whether the GAO or IG has conducted a review of CIP programs. If so, when were these reviews conducted? Were corrective actions identified and follow-on actions taken by the agency? Are corrective actions for IT systems considered critical infrastructure included in Federal Information Security Management Act (FISMA) plans or action and milestones?**

On July 18, 2001, the NRC's Office of the Inspector General (OIG) published report OIG-01-A-13, "Review of NRC's Critical Infrastructure Assurance Program, PDD 63, Phase III." At the time of the audit, the NRC had identified one mission-critical asset, which was the Emergency Telephone System (ETS) in the NRC Operations Center (NRCOC). The audit determined that (1) The 1999 CIPP, the NRC did not pay enough attention to protecting against intrusion and physical damage in the NRCOC, and (2) the NRC's Division of Facilities and Security (DFS) should conduct more frequent vulnerability assessments.

From these results, four recommendations were made to the staff to increase the level of security in the NRCOC:

1. Revise the CIPP [in 2001] to include the NRCOC as a mission critical physical asset.
2. Modify the CIPP to include conducting a vulnerability assessment of the NRCOC every 2 years.
3. Formally document and track the deficiencies resulting from the DFS routine walkarounds of the facility and include the NRCOC.
4. Correct the physical security vulnerabilities in the NRCOC.

On June 25, 2001, shortly after receiving a draft copy of the OIG report and recommendations, the NRC Executive Director of Operations (EDO) issued comments on the CIPP. In these comments, the EDO determined that the NRC does not have any critical infrastructure or mission critical assets as defined in PDD 63. The EDO also committed to revising the CIPP to reflect this determination. The October 2001 CIPP states that the NRC does not have any critical infrastructure as defined in PDD 63. Following this determination, the OIG closed recommendations 1, 2, and 4.

Recommendation 3 was addressed by the EDO in a memo to OIG in August 2001. The EDO noted that DFS would modify its security officer post checklist, used by the DFS staff for routine walkaround inspections, to include the NRCOC and its telephone closets, computer rooms, and other areas that require limited access. The DFS staff continues to conduct walkarounds in the NRCOC on a weekly basis, documenting and tracking deficiencies and corrective actions. OIG continues to periodically follow up with DFS to ensure this commitment is being met.

Since the above recommendation from the OIG audit relates to physical security rather than information security, it was not included in NRC's most recent Federal Information Security Management Act (FISMA) report.

OFFICIAL USE ONLY

Part 2: Provide future plans for protecting critical infrastructure and key resources.

1. **Please attach the prioritized list of internal agency critical infrastructure and key resources. (Prioritization should be conducted based on an analysis and normalization of the risk data - i.e. threats, vulnerability, and consequences)**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

2. **Has the Department/agency developed a long term protective strategy to protect the critical infrastructure and key resources identified above and coordinated sufficiently with other entities, where applicable? Has the IG reviewed this plan? If so, when did this review occur? If weaknesses in the plan were identified, have corrective actions been taken?**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

3. **Has the agency designed and implemented performance metrics for the CIPP program? If so, please provide a copy of the metrics. Activities should be measured both by outputs and by outcomes. Agencies should use the metrics as a basis for improving program activities and reallocating resources as needed.**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

4. **Describe the status of all major initiatives that are underway or planned for addressing deficiencies including:**

- **Improvements to capability to protect critical infrastructure and key resources;**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

- **Improvements to capability to respond to and recover from events that impair the ability to perform organization essential functions at or using critical infrastructure or key resources**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act. However, the NRC COOP Plan is in place to ensure the agency's continued capability to respond to and recover from events that affect minimum essential functions as defined in PDD 67. The COOP Plan is assessed during the following periodic evaluations:

- quarterly tests of the capability to transfer NRCOC telephones to the NRC alternate site
- annual exercises with licensees where the NRC COOP Plan is activated

OFFICIAL USE ONLY

- periodic interagency COOP exercises
- periodic staff training on COOP procedures

Lessons learned and corrective actions are identified based on evaluations of these activities and improvements are implemented aggressively.

- 5. Indicate milestones for the initiatives described in section 3 above. Provide the name of the assigned manager and target date for completing each milestone.**

The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act, so there are no initiative to track.

- 6. Are there specific management, technical, or operational challenges that must be overcome with regard to implementation of the agency's CIPP? How will the agency address these challenges?**

No. The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.

- 7. Has the agency designed and implemented performance metrics for the CIP program? If so, please provide a copy of the metrics. Activities should be measured both by outputs and by outcomes. Agencies should use the metrics as a basis for improving program activities and reallocating resources as needed.**

No. The NRC does not have any critical infrastructure or key resources as defined in the Homeland Security Act and the Patriot Act.