EDO Principal Correspondence Control

FROM: DUE: 05/23/06

EDO CONTROL: G20060484
DOC DT: 05/10/06
FINAL REPLY:

Beth Reed
Department of Homeland Security

TO:

Kane, DEDR

FOR SIGNATURE OF : ** GRN ** CRC NO:

Zimmerman, NSIR

DESC:

Nuclear Sector-Specific Plan
(Comments Due: 5/23/06)

ROUTING:

Reyes
Virgilio
Kane
Silber
Dean
Cyr/Burns
Habighorst,OEDO

DATE: 05/12/06

ASSIGNED TO: CONTACT:

NSIR Zimmerman

SPECIAL INSTRUCTIONS OR REMARKS:

Provide Point-of-Contact from office to Peter Habighorst, OEDO to obtain password to access website. Provide not to Commissioner Assistants via "D" note forwarding response.

OEDO POC: Peter Habighorst

Template: EDO-001

E-RIDS: EDO-01

From: <sspcomments@anl.gov>
To: <wfk@nrc.gov>
Date: 5/10/06 11:16AM
Subject: Nuclear Sector-Specific Plan

Dear Member of the Nuclear Reactors, Materials, and Waste Sector Government Coordinating Council and Sector Coordinating Council:

To fulfill its primary mission to protect the nation's critical infrastructure, the Department of Homeland Security is in the process of finalizing the National Infrastructure Protection Plan (NIPP). The NIPP establishes a common risk-based framework and plan for critical infrastructure protection activities across the 17 critical infrastructure and key resource sectors identified in Homeland Security Presidential Directive 7 (HSPD – 7), Critical Infrastructure Identification, Prioritization, and Protection. The Nuclear Reactors, Materials, and Waste Sector is one of the HSPD-7 critical infrastructures. The attached Nuclear Reactors, Material, and Waste Sector-Specific Plan (SSP) describes the processes to be undertaken in the sector to identify assets, assess risks, establish priorities, develop protective programs, and measure progress.

Your review of the SSP is important to ensure that further stakeholder perspectives on these critical infrastructure protection processes are heard. Although the SSP is a living document that will be reviewed at least annually and reissued at least every three years, we want to ensure that we are off to a good start with this inaugural SSP.

We are very interested in your input on this important document. In order to ensure that your comments are considered, please respond by May 23, 2006.

We recommend that your comments on the draft SSP be submitted through a website specifically established for SSP comments. Instructions for submitting comments to the website at https://comment.iac.anl.gov are provided as a separate attachment entitled Comment Website.

If you choose not to use the website, please use the form provided as a separate attachment entitled Comment Form and mail comments to:

SSPComments - Bldg. 900, MS/12
Argonne National Laboratory
9700 S. Cass Avenue
Argonne, IL 60439

or e-mail comments to: sspcomments@anl.gov.

Any questions on the draft SSP or on submitting comments should be e-mailed to sspcomments@anl.gov or mailed to the above address.

While reviewing the draft SSP, we ask that you focus on issues related to the implementation of its processes in our sector. Please let us know also if there are ways we can clarify how these ideas are presented. We hope the following questions will be helpful to you as a starting point for your review.

What do you see as the desired end state for our sector in terms of protection of assets and a path forward? What current programs exist that contribute to achieving our sector's end state that are not included in the SSP or are not covered adequately? What are possible challenges to achieving the end state that should be addressed in the SSP?

What further information could you provide pertaining to processes and best practices for sector asset definition, processes and methods for conducting vulnerability and risk assessments, and selection/implementation of protective measures?

What information would our sector be willing to share to support the national infrastructure protection

efforts? Examples of such information include asset identification, vulnerability assessments, asset prioritization criteria, risk assessments, etc.

What obstacles, if any, preclude sharing of information? What suggestions do you have for minimizing those obstacles?

What support and guidance does our sector need from the Department of Homeland Security and other parties to help choose and justify appropriate protective measures?

What support and guidance can our sector give to the Department of Homeland Security and other parties to help them choose and justify appropriate protective measures?

What are some specific suggestions on how to create incentives to encourage voluntary participation in the NIPP process by stakeholders?

As mentioned in HSPD-7, each sector is required to submit an Annual Report. DHS recently announced that this reporting process will commence immediately with a deadline of July 1, 2006. Your input will be highly valued to ensure that the Nuclear Sector submits a complete and accurate report which will be fed into DHS' National Report to be submitted to the Executive Office of the President. Please be prepared to receive a draft version of the Annual Report for the Nuclear Sector in early June. It will be sent by email for your review and input.

We are grateful to you for your review of and comments on this SSP as we seek to further sector and national priorities associated with infrastructure protection.

Sincerely,

Beth Reed, Nuclear SSA
Chemical & Nuclear Preparedness
& Protection Division Office of Infrastructure Protection
Department of Homeland Security

Attachments: Sector-Specific Plan Nuclear Reactors, Material, and Waste Sector-Specific Plan (May 2006 Draft)
Comment Website
Comment Form

Mail Envelope Properties (446203B4.378 : 21 : 17272)

Subject: Nuclear Sector-Specific Plan
Creation Date: 5/10/06 11:16AM
From: <sspcomments@anl.gov>

Created By: sspcomments@anl.gov

Recipients
nrc.gov
OWGWPO02.HQGWDO01
WFK (William Kane)

Post Office	Route
OWGWPO02.HQGWDO01	nrc.gov

Files	Size	Date & Time
MESSAGE	5431	05/10/06 11:16AM
comment form.doc	49152	
comment website.doc	35328	
NSSP 2006-05-09.pdf	1201846	
Mime.822	1767429	

Options
Expiration Date: None
Priority: Standard
Reply Requested: No
Return Notification: None

Concealed Subject: No
Security: Standard

Nuclear Sector-Specific Plan Comment Form

(Use only for comments submitted by mail or e-mail)

Step 1: NSSP Individual Commenter Information Submission

Last Name		First Name	
Title		Telephone #	
Organization		Email	

Organization Type	Please Check One	Organization Type	Please Check One
Federal Government		Owner/Operator	
State/ Territory Government		Government Coordinating Council	
Tribal Government		Sector Coordinating Council	
National Association		Non-Profit Organization	
Regional Entity		National Laboratory	
International Entity		Other (specify)	
Private Citizen			

Step 2: NSSP Individual Comment

Page Number (s)	Line Number (s)	Comment Type	Recommended Change	Comment (Required for Critical Comments)

Add additional pages for comments as needed.

Comment Types

- Critical [C] – showstoppers; contentious issue that will cause non-concurrence with specific sections of the document
- Substantive [S] – factually incorrect material
- General [G] - Comment about the document in general. Page and line numbers not required.
- Administrative [A] – grammar, punctuation, style, etc.

Instructions for Using the SSP Comment Website

The preferred method for submitting comments is by using the web based Comment Form which insures that your comments are directly and immediately entered into the database used to collect this information.

To use the website to enter your comments;

- Point your web browser to the website, https://comment.iac.anl.gov
- Your e-mail address acts as your user name. Enter the email address to which this notice was sent, and the password that will be provided to you by telephone, into the boxes on the website. Click on "submit."
  If you have trouble accessing the site, please send an email to: sspcomments@anl.gov
- Complete the comment form:
  - Comment type - select Administrative, Critical, Substantive, or General
  - Page and line number –identify location of text associated with the comment
  - Recommended change – provide text in/text out
  - Comment - provide general comment or justification for critical comment
- The number of comments provided will be displayed as "You have provided "XX" comments."
- Select "submit" and a new comment form will be available; select "review comments" and all comments provided will appear; select "exit" if finished.
- Select "edit" or "delete" to modify comments on comment review page; select "print" to print comments provided; select "Insert additional comment" to return to comment form to add an additional comment; or select "log out" if finished.
- All submitted comment forms will be logged and imported into the Comment Database.

- If the website is not used, please use the attached comment form and mail comments to:

  SSPComments - Bldg. 900, MS/12
  Argonne National Laboratory
  9700 S. Cass Avenue
  Argonne, IL 60439

  or e-mail comments to: sspcomments@anl.gov
- Please e-mail any questions to: sspcomments@anl.gov or mail them to the address above.

Homeland Security

Sector-Specific Plan

Nuclear Reactors, Materials and Waste

for

Critical Infrastructure Protection

As input to the

National Infrastructure Protection Plan

May 2006

DRAFT

DRAFT 05/09/06

Letter of Agreement and Support

The Nuclear Sector-Specific Plan (SSP), along with the overall National Infrastructure Protection Plan (NIPP), provides the unifying structure for the integration of Nuclear Sector protection efforts into a single national program. The NIPP provides the overarching framework to integrate critical infrastructure and key resources (CI/KR) protection programs and activities, and the Nuclear SSP follows the direction of the NIPP and provides the specific framework to integrate Nuclear Sector protection programs and activities. This collaborative effort between the private sector; State, Territorial, local and tribal governments; non-governmental organizations; and the Federal government will result in the prioritization of protection initiatives and investments across the Nuclear Sector to ensure that resources are applied where they offer the most benefit for reducing risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents.

By signing this letter of agreement and support, the Nuclear Sector-Specific Agency (SSA) and other Federal departments and agencies with special function related to Nuclear Sector protection commit to:

- Support Nuclear SSP and NIPP concepts, framework, and processes, and carry out their assigned functional responsibilities regarding the protection of the Nuclear Sector as described within the NIPP and herein.

- Work with the Nuclear SSA, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to coordinate funding and implementation of programs that enhance Nuclear Sector protection.

- Cooperate and coordinate with the Nuclear SSA, in accordance with guidance provided in HSPD-7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate Nuclear Sector protection;

- Develop and modify existing interagency and agency-specific Nuclear Sector plans, as appropriate, to facilitate compliance with the Nuclear SSP and the NIPP.

- Develop and maintain partnerships for Nuclear Sector protection with appropriate State, regional, local, Territorial, tribal, and international entities; the private sector; and non-governmental organizations; and

- Protect Nuclear Sector information containing critical infrastructure information according to the Protected Critical Infrastructure Information (PCII) Program, Safeguards Information (SGI) requirements, or other appropriate guidelines, and share Nuclear SSP and NIPP-related information, as appropriate and consistent with their own agency-specific authorities and the process described within the NIPP and herein.

Signatory departments and agencies follow.

DRAFT

Signatories

Note: This section will contain the listing of the signatories to the Letter of Agreement, including the Director of the Chemical and Nuclear Preparedness and Protection Division (CNPPD) within the Department of Homeland Security.

DRAFT

Letter of Instruction

The Nuclear SSP, in conjunction with the NIPP, provides the overall framework to unify the Nuclear Sector protection efforts into a single national program. This integration effort is a complex task that requires the cooperation of the private sector; State, local, Territorial, and tribal governments; non-government organizations; and the Federal government.

In order for the Nuclear SSP to be successful, the actions described herein must be accomplished. Details on what needs to be done are discussed throughout the Nuclear SSP, and Appendix C contains succinct information on implementation instructions associated with the entire document. All agencies and departments that have signed the Nuclear SSP have committed to carrying out the actions assigned to them. The cooperation of all those involved will result in a even better protected Nuclear Sector than it is today, which will benefit both the nation as a whole and individual Nuclear Sector stakeholders.

DRAFT

Executive Summary

Introduction

Protection of critical infrastructures and key resources (CI/KR) is a necessary component to the overall protection of our homeland. Terrorist attacks as well as unintentional manmade accidents and natural disasters threaten the safety of CI/KR and therefore threaten the economic freedom and way of life that American citizens enjoy. As a first-step towards the large goal of nationwide CI/KR protection, the President issued Homeland Security Presidential Directive 7 (HSPD-7) which called for the establishment of a National Infrastructure Protection Plan (NIPP) to address critical infrastructure protection for all 17 CI/KR sectors.

HSPD-7 assigned responsibility for the protection of CI/KR within each sector to Sector-Specific Agencies (SSAs). The Nuclear Reactors, Materials, and Waste Sector's SSA is the Department of Homeland Security (DHS). Within DHS, the Chemical and Nuclear Preparedness and Protection Division (CNPPD) will maintain responsibility for critical infrastructure protection of the Nuclear Sector.

As each sector is unique in various ways, the SSAs were instructed to create a Sector-Specific Plan (SSP), a complement to the National Infrastructure Protection Plan (NIPP) that will explain how security partners including the private sector; Federal, State, Territorial, tribal and local governments; and international security partners can work together to improve the protection of the Nuclear Sector. The SSP will explain how to identify and prioritize assets, assess risks, and implement protective programs. In order to be sure efforts are garnering results, the SSA will set security goals and measure progress to ensure that those goals are met. This document involved the input of many industry officials, including representatives in the private sector and across government agencies. As a living document, the Nuclear SSP will be reviewed annually and reissued every three years.

By focusing on security from the all-hazards perspective, we can utilize prevention, protection, and response capabilities to not only reduce the threat of a terrorist attack on our nuclear facilities, but to mitigate or prevent damage in the event of a natural disaster or in a case involving human error. While the Nuclear Sector has led the way in implementing robust safety precautions, this comprehensive strategy will help facilitate an even stronger and better protected industry that will be fully prepared to face any challenges that may lie ahead.

1. Sector Profile and Goals

The Nuclear Sector leads the way in sector preparedness with its robust and hardened security system. And yet, considering the hazardous materials used and transported within the Nuclear Sector, it remains one of the most important sectors to protect. Necessary for the overall preparedness initiative is being aware of what constitutes the Nuclear Sector and defining the interdependencies with other sectors upon which the Nuclear Sector depends.

The Nuclear Sector consists of the following facilities. For a more detailed list, please refer to Section 1.1, Table 1.

- Nuclear Power Plants
- Research and Test Reactors

DRAFT

- Nuclear Fuel Cycle Facilities
- Radioactive Waste Management
- Nuclear Materials Transport
- Deactivated Nuclear Facilities
- Radioactive Material Users
- Radioactive Source Production and Distribution Facilities
- Regulatory, Oversight, and Industry Organizations

Two attributes that help make the Nuclear Sector unique are regulation and classification. The NRC independently regulates the sector, with a focus on both security and safety. The amount of focus on both security and safety is rare among the sectors. Significant portions of information on the Nuclear Sector is either classified or protected from disclosure to the general public in some other way, because of the sensitive nature of a variety of information associated with nuclear reactors, materials, and waste. Because of this, there are limitations to the amount of material that can be discussed at certain points in this document.

It is important that the facilities within the Nuclear Sector are aware of any dependencies they may have on other sectors. For example, the Nuclear Sector relies on the transportation sector for shipping nuclear and radiological materials and the energy sector for its supply of electrical power. By working to implement any dependencies into a preparedness plan, each nuclear facility can plan for the impact of problems in other sectors upon that facility's operation. For instance, if there was a power outage in a city or region, the affected nuclear facility should become aware of it and make adjustments to its operation accordingly. By becoming mindful of such dependencies and working with the SSA to facilitate cross-sector communication, the nuclear sector can be better prepared to respond to a variety of disruptions to the activities of each facility.

The DHS Strategic Plan describes the full spectrum of protection activities, which includes awareness, prevention, protection, response, and recovery. The Nuclear SSP goals range across all these areas. The eight Nuclear SSP goals are:

- Goal #1[1] - Establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities.
- Goal #2 - Determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector.
- Goal #3 - Prevent nuclear and radioactive material from being used for malevolent purposes.
- Goal #4 - Coordinate with Federal, State, and local Law Enforcement Agencies to develop tactics to deter, detect and prevent terrorist attacks on fixed nuclear facilities.
- Goal #5 – Protect the cyber assets of the nuclear sector from being exploited.
- Goal #6 – Utilize R&D to better protect the Nuclear Sector from future threats.

[1] The numbering of the goals is not to identify priorities, but is for identification purposes only.

DRAFT

- Goal #7 – Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.
- Goal #8 – Enhance the ability of the Federal, State, Territorial, tribal, local, and private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents.

2. Identify Assets, Systems, Networks, and Functions

In order to eventually initiate protective measures within a sector, DHS needs to first understand what assets, systems, networks, and functions are contained within the sector. The National Asset Database (NADB) was created in order to collect and store asset information. The NADB is an extensive inventory of information for assets in all 17 CI/KR sectors. Information has historically been gathered through DHS-initiated data calls and through the cooperation of owners and operators. Additionally, the NRC will begin sharing its own nuclear asset data with DHS. When appropriate, marking information as Safeguards Information (SGI) or utilizing the Protected Critical Infrastructure Information (PCII) Program will keep data from being improperly disclosed.

3. Assess Risks

Risk is a function of threat, vulnerability, and consequence. In order to efficiently utilize limited resources in protecting assets, DHS needs to be able to understand what risk the asset faces in comparison with the risk associated with other assets, in order to make the best determination on what assets to protect and how to protect them. In characterizing threat, DHS will consider modes of attacks at a nuclear facility, threats using stolen items diverted from a facility, and possible breaches of a facility's cyber system. Vulnerability assessments will determine areas of an asset that may be penetrable to a specific threat. Consequence assessments will determine the likely damage resulting from a perceived threat and includes mass casualties, financial impacts, and economic disruptions. By evaluating consequences, vulnerabilities, and threats, DHS and industry can work together to protect assets that have the most risk.

4. Prioritize Infrastructure

Risk Analysis and Management of Critical Assets Protection (RAMCAP) is a program developed by industry with assistance from DHS to create guidelines for both the threat, vulnerability, and consequence assessments as well as for comparing and prioritizing assets across all sectors. RAMCAP successfully utilizes the consequence/vulnerability/threat equation by considering the consequences of a successful attack, the asset's vulnerability to the attack, and the likelihood of the attack occurring to give a numerical score to an asset. In addition to this equation, RAMCAP takes cross-sector interdependencies into account. With a significant overlap between sectors, it is important to realize that the consequences of a successful attack affect more sectors than the one containing the facility that was attacked. Ultimately, by successfully prioritizing assets, DHS, industry, and other security partners can most efficiently utilize limited resources in protecting those assets that need the most protection.

DRAFT

5. Develop and Implement Protective Programs

A protective program is a coordinated plan of action to prevent, deter, and mitigate terrorist attacks on critical assets, and to respond to and recover from such acts as quickly and effectively as possible. DHS has worked with many government and industry representatives to develop and coordinate programs that have been effective thus far in assisting the protection effort of our nation's CI/KR. Additionally, the Nuclear Sector is already very well protected and contains a wealth of information regarding best practices and security measures. DHS hopes to facilitate further discussion within the sector to share lessons learned and best practices to encourage implementation of the effective security measures some facilities in the Nuclear Sector already employ as well as some of the DHS-initiated programs.

6. Measure Progress

Within the Nuclear SSP Working Group, representatives of government, industry, and DHS worked to create a robust set of goals, objectives, and metrics that can be used to measure the progress of the Nuclear Sector in its critical infrastructure protection (CIP) efforts. By identifying goals and creating metrics to measure them, the Nuclear Sector will have an accomplishable plan to protect the Nuclear Sector. Additionally, by reporting on the sector progress in meeting the metrics, the SSA can identify gaps in protection and work to repair them.

7. CI/KR Protection R&D

Much of this Nuclear SSP addresses work that is being done currently or in the near future to protect the Nuclear Sector from terrorist attacks, natural disasters, and manmade accidents. Yet, there is a long road still ahead in order to achieve an even more secure sector and continue to deter terrorist activity. Some key elements to long-term Nuclear Sector protection are: awareness, training and education; Research and Development (R&D) initiatives; and ongoing planning, management, and resource allocation. These long-term endeavors will require the various Nuclear Sector stakeholders to continue to work together. With persistent efforts, the Nuclear Sector will continue to improve its security posture and maintain its reputation as a leading sector in security.

8. Managing and Coordinating SSA Responsibilities

As the SSA, CNPPD has many responsibilities for the Nuclear Sector. The SSA will be responsible for monitoring protective program requirements, working to fill gaps in programs or resources and ensuring the sector meets its goals and objectives. Additionally, the SSA will play a large role in facilitating communication between sector security partners to make certain best practices are shared and dependencies and interdependencies are identified and incorporated into preparedness plans. The SSA will also be responsible for submitting an Annual Report on CI/KR Protection to the Secretary of Homeland Security by July 1. This report will be used to compile the National CI/KR Protection Report to be presented to the President on an annual basis.

DRAFT

Table of Contents

Letter of Agreement and Support 1

Signatories 2

Letter of Instruction 3

Executive Summary 4

Introduction 4

1. Sector Profile and Goals 4

2. Set Security Goals ..... **Error! Bookmark not defined.**

3. Identify Infrastructure 6

4. Assess Risks 6

5. Prioritize 6

6. Implement Protective Programs 7

7. Measure Progress 7

8. Long-Term Sector CI/KR Protection Elements 7

Table of Contents 8

Introduction 12

Purpose 12

Goals and Objectives 15

Nuclear Sector Security Goals 16

Planning Assumptions 17

Review of Authorities 17

1 Sector Profile and Goals 19

1.1 Sector Profile 21

1.1.1 Reactors 22

1.1.2 Materials and Waste 24

1.1.3 Decommissioning 32

1.1.4 The Human Element 32

1.1.5 The Cyber Element 33

1.1.6 Interdependencies and Overlapping Relationships with Other Sectors 33

1.2 Security Partners 35

1.2.1 Nuclear Sector Entities ..... **Error! Bookmark not defined.**

1.3 Sector Security Goals 44

1.3.1 Elements and Characteristics of Sector Security Goals 44

1.3.2 Process to Establish Sector Security Goals 48

1.3.3 Cross-Sector Initiatives 49

DRAFT

1.4 Value Proposition 49
1.5 Challenges 50
1.6 Initiatives 50

2 Identify Assets, Systems, Networks, and Functions 54
2.1 Defining Information Parameters 55
2.2 Collecting Infrastructure Information 57
2.2.1 DHS Data Collection for NADB 58
2.2.2 Future DHS Data Collection Efforts within the Nuclear Sector 59
2.2.3 Use of Infrastructure Information 59
2.3 Verifying Infrastructure Information 59
2.3.1 Review of Submitted Material 60
2.3.2 Inspection Process 60
2.3.3 Data on Radioactive Materials 60
2.4 Updating Infrastructure Information 61
2.5 Protecting Infrastructure Information 61
2.5.1 PCII Program 61
2.5.2 Classified Information 62
2.5.3 Safeguards Information (SGI) 62
2.6 Challenges 63
2.6.1 Materials Tracking/Inventory 63
2.6.2 Telecommunications Dependencies 63
2.7 Initiatives 63

3 Assess Risks 65
3.1 Use of Risk Assessment in the Sector 65
3.1.1 Risk Analysis and Management of Critical Assets Protection (RAMCAP) 66
3.1.2 NRC Process 69
3.1.3 Cyber Security in the Nuclear Sector 70
3.1.4 Securing Risk Assessment Information 71
3.2 Screening Infrastructure 71
3.2.1 RAMCAP Screening 71
3.2.2 NRC Screening 71
3.3 Assessing Consequences 73
3.3.1 Assessment Methodology 74
3.3.2 Aircraft Attack at a Nuclear Power Plant 75
3.3.3 Assessing Emergency Planning in Determining Consequences 75
3.3.4 Radiological Dispersal Device (RDD) 76
3.3.5 Industrial and Medical Facilities That Use Risk-significant Radioactive Sources 77
3.3.6 Radioactive Material Transportation Packages, and Radioactive Waste and Storage 77
3.3.7 Research and Test Reactors 78
3.3.8 Other Industrial and Medical Facilities 78
3.3.9 Tools for Assessing the Consequences of a Radiological Event 79

DRAFT

3.4 Assessing Vulnerabilities 79
3.4.1 Engineering Analysis of Nuclear Facility Vulnerabilities 79
3.4.2 Radioactive Material Users and Sources (Radioactive Materials in Quantities of Concern) 81
3.4.3 Transportation of Risk-significant Radioactive Sources 81
3.5 Assessing Threats 82
3.5.1 Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) 84
3.6 Challenges 84
3.6.1 Cyber 84
3.6.2 Physical 84
3.7 Initiatives 85
4 Prioritize Infrastructure 88
4.1 Process to Prioritize Infrastructure 88
4.1.1 DHS Efforts to Prioritize Infrastructure 89
4.1.2 Other Sector Efforts to Prioritize Infrastructure 90
5 Develop and Implement Protective Programs 92
5.1 Overview of Sector Protective Programs 94
5.2 Determining Protective Program Needs 95
5.2.1 Decision-Making Processes 95
5.3 Protective Program Implementation 97
5.3.1 Protective Program Implementation ..... **Error! Bookmark not defined.**
5.3.2 NRC Rulemaking 107
5.4 Protective Program Performance 108
5.5 Challenges 108
5.5.1 Integrated Response 108
5.5.2 Reactor Licensees 108
5.5.3 Control of Radioactive Materials in Quantities of Concern 109
6 Measure Progress 110
6.1 CI/KR Performance Measurement 110
6.1.1 Developing Sector-Specific Metrics 111
6.1.2 Information Collection and Verification 116
6.1.3 Reporting 117
6.2 Implementation Actions 117
6.3 Challenges and Continuous Improvement 118
7 CI/KR Protection R&D 120
7.1 Overview of Sector R&D 120
7.2 Sector R&D Requirements 120
7.3 Sector R&D Plan 121
7.3.1 Current R&D Initiatives 121

DRAFT

7.3.2 Gaps 123
7.3.3 Planned R&D Initiatives 123
7.4 R&D Management Processes 123

8 Managing and Coordinating SSA Responsibilities 125
8.1 Program Management Approach 125
8.2 Processes and Responsibilities 125
8.2.1 SSP Maintenance and Update 125
8.2.2 Annual Reporting 125
8.2.3 Resources and Budgets 126
8.2.4 Training and Education 126
8.3 Implementing the Sector Partnership Model 127
8.3.1 Coordinating Structures 127
8.4 Information Sharing and Protection 131
8.4.1 Homeland Security Information Network 131
8.4.2 Operation Centers 132

List of Acronyms and Abbreviations 136

Glossary of Terms 141

1 Authorities 143
Department of Homeland Security 143
Department of Transportation 145
Nuclear Regulatory Commission 145
Federal Bureau of Investigation (FBI) 147

2 Sector Protective Programs 148
Initiatives 148
Integrated Response 148
Reactors and Spent Fuel Facilities 148
Radioactive materials in quantities of concern 150
Information Security 151

Tables

Table 1: Nuclear Facilities Sector 21
Table 2: List of NRC Agreement States 31
Table 3: Nuclear Sector Interdependencies and Overlaps With Other CI/KR Sectors ..... **Error! Bookmark not defined.**
Table 4: Nuclear Facilities Sector 55

DRAFT

Introduction

The ultimate goal of the national critical infrastructure protection (CIP) program is to protect the Nation's critical infrastructure/key resources (CI/KR), a responsibility that is shared among the private sector; State, local, tribal, and Territorial governments; and the Federal government. The Homeland Security Act, and the subsequent Presidential strategies on critical infrastructure protection, defined what must be done to protect the Nation's CI/KR, but they did not define how this would be accomplished. To provide the overall guidance for further developing and implementing this national CIP program, the President issued Homeland Security Presidential Directive 7 (HSPD-7).

A key requirement of HSPD-7 is development of the National Infrastructure Protection Plan (NIPP), which describes the activities to:

- Identify CI/KR assets
- Reduce the vulnerability of CI/KR assets
- Prioritize CI/KR (as a basis for resource allocation)
- Coordinate the protection of CI/KR
- Share information on CI/KR

HSPD-7 recognizes that CI/KR sectors possess unique characteristics and operating models, and assigns CIP responsibilities for those sectors to sector-specific agencies (SSAs), with guidance to be provided by the Department of Homeland Security (DHS). To implement HSPD-7, SSAs were instructed to develop Sector-Specific Plans (SSPs) that provide an informational foundation for the NIPP.

Development of the NIPP is an ongoing, evolving process that requires the participation of all stakeholders from the private sector, the SSA, and Federal, State, Territorial, local, and tribal governments. The NIPP provides an overall framework that incorporates existing CIP programs that have been underway both within DHS and throughout the various CI/KR sectors. As these CIP efforts and programs are developed, implemented, and refined, the NIPP will be updated to reflect this progress.

Purpose

The NIPP requires each critical infrastructure and key resource sector to develop a Sector-Specific Plan (SSP) with the purpose of providing a framework for reducing risk and fostering cooperation and information sharing between security partners, including all levels of government, the private sector, and international organizations. The Sector-Specific Agencies (SSAs) are responsible for the development of the SSP, in coordination with the security

DRAFT

partners. The nuclear SSP will follow and support the same risk management approach and key steps as the NIPP:

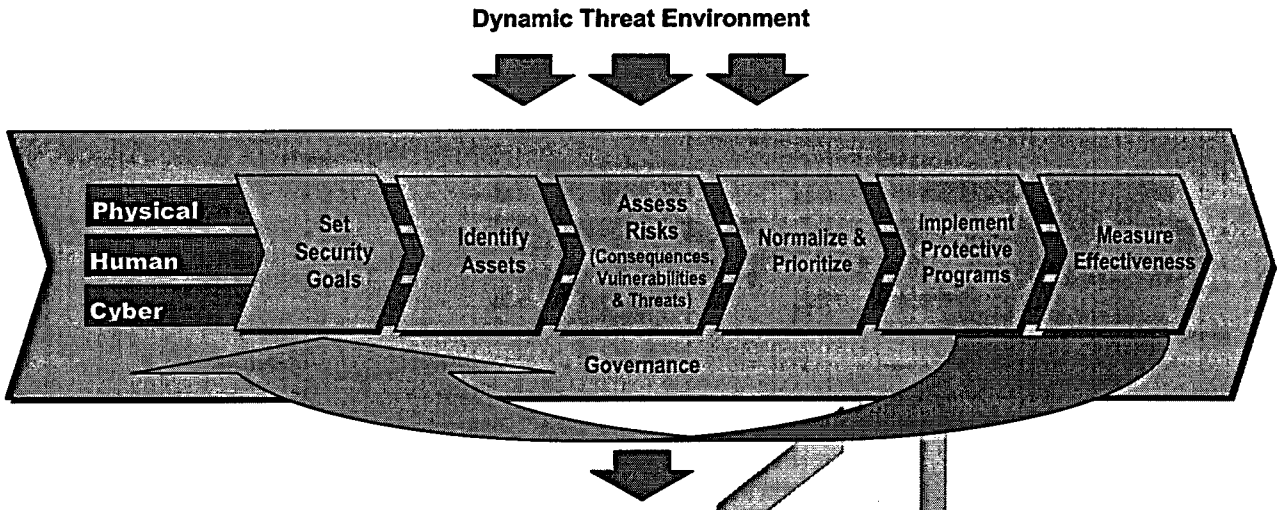
- Setting security goals
- Identifying the sector's CI/KR assets, systems, networks, and functions
- Identifying and assessing the vulnerabilities and interdependencies among CI/KR assets, and analyzing potential risks based on threats and consequences
- Prioritizing assets based on an analysis and normalization of vulnerability data and prioritizing protection initiatives based on costs and benefits so that they are used where they offer the greatest reduction of risk
- Developing sustainable programs to protect assets and implementing these programs when necessary
- Implementing information sharing and protection measures within and across CI/KR sectors
- Using metrics to measure and communicate the effectiveness of the SSP

As there has been a process established for the review and maintenance of the NIPP, the SSP will also undergo a similar process to ensure that preparedness efforts remain strong and current. This review process will include input from many industry officials, including representatives in the private sector and across government agencies and the SSP will be reviewed annually and reissued every three years.

Exhibit 1, also known as the Risk Management Framework, shows these activities being implemented based on a dynamic threat environment, with threat information provided by DHS. The resulting outputs are sector-specific strategies to protect assets. The ultimate objective of this SSP is to have the Federal, State, Territorial, local, tribal, and private sectors work with the SSA to implement the plan in a way that is consistent, sustainable, effective, and measurable.

Exhibit 1: Sector-Specific Plan Development and Implementation

DRAFT



This SSP provides a detailed description of the specific processes that are used to identify, assess, prioritize, and protect CI/KR; processes used to measure effectiveness; the plans for implementing these processes, including lists of projects, initiatives, activities, time frames, milestones, and resource limitations; and the status of any efforts being conducted to support this effort to date, including best practices identified, challenges encountered, and products generated. This SSP also realizes that a successful terrorist attack, such as one that employs a weapon of mass destruction, could cause catastrophic health effects or mass casualties and this document intends to help protect the Nuclear Sector from such an event. At the same time, CI/KR protection uses the all-hazards approach which aims to protect infrastructures from natural disasters and unintentional human errors as well as a potential terrorist attack.

Nothing in this SSP alters, or impedes the ability of Federal departments and agencies to perform their responsibilities under law. This SSP enables Federal, State, Territorial, tribal, and local governments and the private sector to work together in the protection of the Nuclear Reactors, Materials, and Waste Sector.

Scope and Applicability

Per the guidance of the NIPP, the nuclear SSP focuses on the protection of the nuclear sector from the impact of a possible terrorist attack while recognizing that in doing do, the sector is also acting in compliance with the Nation's all-hazards approach. This would increase overall preparedness so as to help manage the effects of a natural disaster or unintentional man-made incident in the same preparedness measures taken in respect to terrorism. These protective measures are necessary and must be addressed in multiple contexts including international vulnerabilities and cross-sector partnerships. Additionally, HSPD-7 directs the protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste.

This document is applicable to the following nuclear subsectors. For a more detailed list, please refer to Section 1.1, Table 1.

- Nuclear Power Plants
- Research and Test Reactors
- Nuclear Fuel Cycle Facilities
- Radioactive Waste Management
- Nuclear Materials Transport
- Deactivated Nuclear Facilities
- Radioactive Material Users
- Radioactive Source Production and Distribution Facilities
- Regulatory, Oversight, and Industry Organizations
- Other Nuclear Facilities

Goals and Objectives

The ultimate goal outlined in the NIPP is to: *enhance protection of the Nation's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enable national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.* The following goals are actions that the nuclear sector can take to help achieve the goals specified in the NIPP.

DRAFT

Nuclear Sector Security Goals		
Risk Management Steps	**Goal**	**Office(s) of Responsibility** **Primary – (P)** **Support – (S)**
Awareness	#1 – Establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities.	NRC – P DHS – P
	#2 – Determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector.	DHS/RMD – P
Prevention	#3 – Prevent nuclear and radioactive material from being used for malevolent purposes.	DHS/DNDO – P
	#4 – Coordinate with Federal, State, and local Law Enforcement Agencies to develop tactics to deter, detect and prevent terrorist attacks on fixed nuclear facilities.	DHS/RMD – P
Protection, Response, and Recovery	# 5 – Protect the cyber assets of the nuclear sector from being exploited.	DHS/CNPPD – P
	#6 – Utilize R&D to better protect the Nuclear Sector from future threats.	DHS – P
	#7 – Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.	DHS/CNPPD – P

DRAFT

	#8 – Enhance the ability of the Federal, State, Territorial, tribal, local, and private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents.	DHS/CNPPD – P

Planning Assumptions

- The nuclear sector is dependent on other sectors for its full operation and in many cases, a failure in another sector may affect the ability of the nuclear sector to perform its necessary functions.
- CI/KR protection requires participation and communication of all stakeholders.
- CI/KR protection activities take place in a highly dynamic threat environment, which changes as the capabilities and the intentions of terrorists evolve.
- Given the uncertain nature of the terrorist threat, the full range of threats, not just the most likely or those involving the most frequent reporting, must be regarded when considering actions to enhance CI/KR protection.
- It is not practical to protect all assets, systems, networks, and functions against every possible terrorist attack. A risk-based approach driven by intelligence analysis and reporting is crucial to an effective risk management strategy and efficient resource allocation.
- Successful CI/KR protection requires robust baseline information on assets, systems, networks, and functions within and across CI/KR sectors, regions, and specific localities.
- Owners and operators conduct risk management planning and invest in security from a business perspective.
- Efforts to enhance CI/KR protection from a terrorist attack also support all-hazards preparedness and response, including threats such a natural disasters and unintentional man-made hazards.
- Unlike many other sectors, the Nuclear Sector also has an independent regulator, the NRC.

Review of Authorities

Protection of the assets, systems, networks, and functions defined in this sector requires activities that entail a high level of cooperation and coordination among diverse entities in the public and private sectors. Numerous legal authorities govern these activities. Agencies with authorities within the nuclear sector are listed below. For full information and details on the assigned authorities, please refer to Appendix 1.

Department of Homeland Security – DHS creates and oversees the programs and procedures to identify, prioritize, and protect CI/KR assets, systems, networks, and functions. This includes coordinating security efforts with stakeholders, identifying gaps and vulnerabilities, and facilitating the sharing of lessons learned and best practices.

Department of Transportation – DOT is responsible for ensuring safe and protected transport of hazardous materials in intrastate, interstate, and foreign commerce.

DRAFT

Nuclear Regulatory Commission – The NRC has the authority to regulate radioactive materials and activities within the nuclear sector, including the shipping and storage of nuclear materials outside the United States.

Federal Bureau of Investigation – The FBI is responsible for working with the law enforcement community to help detect and prevent terrorist attacks within the nuclear sector through its authority to conduct criminal investigations.

DRAFT

1 Sector Profile and Goals

This sector includes the Nation's 104 commercial nuclear power reactors, which are licensed to operate in 31 states. Nuclear power accounts for approximately 20 percent of the Nation's electricity-generating capacity. Nuclear power plants are among the best-defended and most physically hardened of the critical infrastructures in the country, designed to withstand such extreme events as hurricanes, tornadoes, tornado-generated missiles, and earthquakes. While losing the electricity generated by a single nuclear power plant may have only a minor impact on the Nation's overall electrical capacity, an event, such as a terrorist attack, would be considered a significant security event. In an unlikely scenario, a successful terrorist strike could result in the release of radioactive material[2].

As noted in paragraph 29 of HSPD-7, this sector, designated as one of the nation's key resources, encompasses more than just commercial nuclear power reactors. It includes: "(1) commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; (2) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and (3) the transportation, storage, and disposal of nuclear materials and radioactive waste." The "nuclear materials" referenced in items 2 and 3 include source, byproduct, and special nuclear material[3]. Decommissioned reactors are also part of the sector. One reason why nuclear materials are important is that, if stolen, certain materials may be used in attacks against other CI/KR, or against the public. Therefore, this plan goes beyond just covering commercial nuclear power reactors, but also encompasses the remainder of the sector as defined in HSPD-7.

The SSA responsible for protection of the Nuclear Reactors, Materials, and Waste Sector is DHS. Within DHS, the Chemical and Nuclear Preparedness and Protection Division (CNPPD) has been assigned this responsibility. The Nuclear Regulatory Commission (NRC) has the authority to regulate reactors, materials, and waste pursuant to the Atomic Energy Act of 1954, as amended. HSPD-7, paragraph 29 states that the Secretary of Homeland Security "will continue to work with the NRC and, as appropriate, the Department of Energy (DOE) in order to ensure the necessary protection of" this sector.

This plan is the result of the combined effort of the public and private sectors. Within the public sector, the NRC, DOE, the Department of Transportation (DOT), the Federal Bureau of Investigation (FBI), and numerous parts of DHS made valuable contributions. The contribution from the private sector was just as important, and included cooperation and inputs from the industry's owner/operator licensees and the Nuclear Energy Institute (NEI).

For more than 25 years, reactor and fuel cycle facility licensees have implemented rigorous security and emergency response programs required by the NRC. Because there is a graded regulatory approach to security that is generally consistent with potential risks from these materials, prior to September 11, 2001, comprehensive security plans were not required at all fuel cycle facilities. Immediately after September 11, 2001, the NRC issued a series of safeguards and threat advisories to its major licensed facilities, placing them on the highest

[2] Radioactive Material - Material that undergoes spontaneous emission of radiation (alpha, particles, beta particles and gamma rays) directly from unstable atomic nuclei.

[3] Special Nuclear Material – Uranium-233 or uranium-235, enriched uranium, or plutonium

security level, and advising them to take additional security measures. Licensees responded by implementing significant voluntary measures to enhance the security of their facilities. These actions enhanced security across the nuclear industry, and many of the enhanced security measures are now requirements as a result of subsequently issued NRC security orders. The security enhancements include measures to provide additional protection against vehicle bombs, as well as water- and land-based assaults.

Also, when determining what protective measures the sector should have in place, consideration needs to be given to the possibility that certain protective measures could reduce the benefits that the sector provides to the American people. For instance, security protective measures that could impede the movement of radioactive materials could potentially impact the supply chain for time-sensitive medical isotopes subsequently affecting thousands of patients in need of diagnostic and therapeutic administration. If specific protective measures result in a reduction of the sector's benefits to the American people, that needs to be considered as part of the cost in implementing the protective measure.

This sector has interdependencies with other sectors, including the energy sector as a supplier to the Nation's electrical grid; the transportation sector through the movement of radioactive materials; the chemical industry and hazardous materials sector related to hazardous chemicals at fuel cycle facilities; public health through nuclear medicine, radiopharmaceuticals, and sterilization of surgical supplies; and the government facilities sector through Federal and State facilities that use radioactive material for a myriad of purposes. While nuclear power plants provide electrical power to the grid, infrastructure protection for the grid will be discussed in the Energy SSP. This Nuclear Reactors, Materials, and Waste SSP will discuss the grid only as it relates to nuclear power plant operations and vulnerabilities. The sector does not include Department of Defense (DOD) and DOE nuclear facilities or radioactive materials associated with defense related activity. However, the sector does include DOE Research and Test Reactors (RTRs).

Two attributes that help make the Nuclear Sector unique are regulation and classification. The NRC independently regulates the sector, with a focus on both security and safety. The amount of focus on both security and safety is rare among the sectors. Significant portions of information on the Nuclear Sector is either classified or protected from disclosure to the general public in some other way, because of the sensitive nature of a variety of information associated with nuclear reactors, materials, and waste. Because of this, there are limitations to the amount of material that can be discussed at certain points in this document.

The Nuclear Reactors, Materials, and Waste Sector is also referred to as the Nuclear Sector. This document, the Nuclear Reactors, Materials, and Waste SSP, is also referred to as the Nuclear SSP.

DRAFT

1.1 Sector Profile

The National Asset Database (NADB), which will be discussed further in Chapter 2, utilizes a taxonomy to divide the Nuclear Sector into subsectors. This taxonomy[4], which is detailed below, gives a good high-level overview of the sector's profile.

Table 1: Nuclear Sector

NUCLEAR POWER PLANTS
- A. Light Water Reactor Power Plants
- B. Other Reactor Power Plants

RESEARCH AND TEST REACTORS
- A. Government Research and Test Reactors
- B. University Research and Test Reactors
- C. Private Research and Test Reactors

NUCLEAR FUEL CYCLE FACILITIES
- A. Uranium Mining or In Situ Uranium Leaching
- B. Uranium Ore Milling or Leachate Processing
- C. Uranium Conversion Facilities
- D. Uranium Enrichment Facilities
- E. Fuel Fabrication Facilities
  - 1. Category I (Special Nuclear Materials) Facilities
  - 2. Category II (Special Nuclear Materials – Moderate Strategic Significance) Facilities
  - 3. Category III (Special Nuclear Materials – Low Strategic Significance) Facilities

RADIOACTIVE WASTE MANAGEMENT
- A. Low-Level Radioactive Waste Processing and Storage Facilities
- B. Sites Managing Accumulations of Naturally Occurring Radioactive Materials (NORM)
- C. Spent Nuclear Fuel Processing and Storage Facilities
  - 1. Spent Nuclear Fuel Wet Storage Facilities
  - 2. Spent Nuclear Fuel Dry Storage Facilities
- D. Transuranic Waste Processing and Storage Facilities
- E. High-Level Radioactive Waste Storage and Disposal[5] Facilities

NUCLEAR MATERIALS TRANSPORT
- A. Low Hazard Radioactive Materials Transport
- B. High Hazard Radioactive Materials Transport

DEACTIVATED NUCLEAR FACILITIES
- A. Deactivated Reactors
- B. Other Deactivated Nuclear Facilities

RADIOACTIVE MATERIAL USERS
- A. Medical Facilities with Radioactive Materials
- B. Research Facilities with Radioactive Materials
- C. Irradiation Facilities
- D. Industrial Facilities with Nuclear Materials
- E. Radiopharmaceutical and Medical Isotope Production Facilities
- F. Radiographers, Well Loggers, and Portable Density Gauge Users[6]

RADIOACTIVE SOURCE PRODUCTION AND DISTRIBUTION FACILITIES
- A. Radioactive Source Importers
- B. Radioactive Source Manufacturers

DRAFT

[4] The order in which the various subsectors are listed does not reflect the amount of risk, threat, vulnerability, or consequence associated with these types of assets in regard to a terrorist attack.

REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
- A. Federal Nuclear Agencies
- B. Regional, State, and Local Nuclear Agencies
- C. Nuclear Industry Organizations

OTHER NUCLEAR FACILITIES

1.1.1 Reactors

1.1.1.1 U.S. Commercial Nuclear Power Reactors

The NRC licenses 104 commercial nuclear power reactors to operate at 65 sites in 31 States. Although there are many similarities, each reactor design can be considered unique, in that there are:

- 4 reactor vendors
- 41 licensees
- 80 designs
- 65 sites

Commercial nuclear power plants in this country can be owned by a number of separate entities, each with varying ownership proportions. Each of these owners may, in turn, have a parent/subsidiary relationship with other companies. The operator of the plant may be a different entity, as well. The report, NRC NUREG-1350, United States Nuclear Regulatory Commission Information Digest, published annually in August, provides a compilation on the owners/operators for all commercial power reactors in the United States.

A nuclear facility with a single power reactor may have a staff of approximately 400-500 personnel, depending on the organizational structure. Some sites have two, or even three power reactors, with staffing levels up to 1,500 people. Staffing consists of operations, maintenance, engineering, technical support, management, and security personnel.

A nuclear power plant is an arrangement of structures, systems, and components used to generate electric power. The following are some major components common to all current U.S. nuclear power plants and their functions:

- Nuclear reactor cores produce energy to heat water.
- Reactor vessels house and provide for proper control of the reactor core.
- Containment structures and systems prevent the release of radioactivity to the environment in the event that the reactor coolant system and reactor core are damaged.

[5] For item E under "radioactive waste management", the NADB currently states "High-Level Radioactive Waste Storage Facilities." However, a modification plans to be made so item IV.E reads "High-Level Radioactive Waste Storage and Disposal Facilities."

[6] Items E and F under "radioactive material users" have not yet been added to the NADB, but will likely be added in the near future.

- Heat transfer/working fluid loops transfer power from the reactor to electricity-generating components.
- Heat sinks (e.g., cooling tower, river, lake, ocean) and associated normal cooling water systems provide for condensing steam and cooling plant equipment during normal operation.
- Plant control room and reactor control systems allow for proper control of the reactor under normal and emergency conditions.
- Pools and casks store spent nuclear fuel.
- Turbine generators convert heat in the steam to electrical power.
- Generating transformers convert electricity into usable form for transmission and consumption.
- Transmission lines and downstream substations deliver electricity from the power plant to consumers.

Nuclear power plants also have the following to allow for accident mitigation:

- Through safety features included in the nuclear power plants' design and safety procedures that are followed, the ability to prevent, or mitigate the impact of, damage associated with a robust series of design basis accidents. These design basis accidents cover a broad spectrum of situations such as, earthquakes, fires, floods, loss of offsite power, extreme winds such as hurricanes and tornadoes, and others.
- Three distinct barriers that are designed to prevent radioactive materials from being released. These are the fuel pins that contain actual fuel pellets, the reactor vessel itself where the fuel resides that is made from many inches of high strength steel, and the containment building that encloses the reactor components that is made of heavily reinforced concrete many feet thick. All of these are designed to prevent the release of radioactive materials from fuel pellets.
- Redundant emergency systems with redundant electrical power, designed to preclude overheating and melting of the core and the release of radioactive material during an accident.
- Redundant instrumentation and control (I&C) features that automatically initiate reactor shutdown and emergency systems activation in the event of an accident.
- Emergency plans and procedures, and severe accident management strategies, designed to reduce accident consequences and minimize the public's radiation exposure.
- Strong training programs and frequent emergency plan testing that is integrated with local, State, and Federal sector involvement designed to ensure that the emergency response organizations are well tested.

1.1.1.2 Research and Test Reactors (RTRs)

Thirty-three RTRs are licensed by the NRC to operate in 23 states. RTRs—also called nonpower reactors—are nuclear reactors used primarily to conduct research, to develop theoretical practices, and for education or medical purposes. Most of these RTRs are at

DRAFT

universities or colleges in the United States, while several others are operated by private companies and the Federal Government.

RTRs are typically licensed according to the total thermal (heat) energy produced by the reactor. These facilities range in size from 0.10 watt to 20 megawatts (thermal). In contrast, a typical commercial nuclear power reactor is rated at 3,000 megawatts (thermal). Because of this large difference in power generated, the consequence of an accident at a RTR is limited when compared to that at a commercial power reactor. For this reason, adequate emergency planning zones to protect the public from potential radiological accidents at RTRs are typically well within owner-controlled areas, often only to the boundary of the room in which the reactor is housed.

Research and tests reactors take many varieties and forms. Reactors may be classified by the type of material—called the moderator—used to slow the neutrons that cause fission. Typical moderators include water (H_2O), heavy water (D_2O), polyethylene, and graphite.

All NRC-licensed RTRs have a built-in safety feature that reduces reactor power during potential accidents before an unacceptable power level or temperature is reached.

Unlike power plants, RTR control rooms are usually in the confinement or containment area that houses the reactor; facility staff and personnel work in the reactor room or building during operation. Most RTRs are in rooms or buildings that have dedicated ventilation systems. Some RTRs have confinement areas that maintain negative pressure with respect to the surroundings; ensuring that any radioactive material released from the reactor is controlled. Others have a containment area that can control potential over-pressure conditions.

All RTRs have fail-safe shutdown systems. Before an unsafe condition occurs, control rods rapidly shutdown the reactor. Redundant systems that initiate a reactor shutdown also help to protect the public. Most of the reactors do not generate enough heat to be of concern in the event of a loss-of-coolant accident. Others have auxiliary features and systems capable of adding water to provide core cooling; the source of water can be a water tank, or city water. Because of the low power levels at which RTRs operate, they only require this cooling for short periods after shut down. Many of these RTRs are located in pools, under a significant amount of water. There is little likelihood that the energy release or radiation release outside the pool could harm the public.

1.1.2 Materials and Waste

1.1.2.1 U.S. Fuel Cycle Facilities

There are seven major fuel fabrication and production facilities licensed by the NRC to operate in six states. In addition, the NRC regulates two gaseous diffusion fuel enrichment facilities, one operating and one in cold standby, which are operated by the United States Enrichment Corporation (USEC) and leased from DOE. The NRC regulates nine additional facilities (other than reactors) that possess significant quantities of special nuclear material or process source

DRAFT

material[7] (other than uranium recovery facilities, where uranium is extracted from the ground or from mined ore).

The principal hazards at fuel cycle facilities are from chemical releases. The offsite releases from these chemicals can have substantially greater consequences than the associated radioactive materials, even as compared to radioactive releases from reactors. The Environmental Protection Agency (EPA) has Coordinating Agency responsibilities for hazardous materials in accordance with the National Response Plan (NRP).

Fuel cycle facilities are categorized based upon the type of nuclear material[8] stored or produced at the site. Special nuclear material is given different designations, depending upon its level of enrichment and the amount of material possessed by the facility. The three categories are defined as:

1. Category I Fuel Cycle Facilities

   A. Licensed to receive, possess, use, and store a Category I quantity of strategic special nuclear material (SSNM). SSNM consists of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium

   B. A Category I quantity of SSNM is 5,000 grams or more of SSNM in any combination computed by the formula

      grams = (grams contained U-235) + 2.5 (grams U-233+grams plutonium)

   C. Currently, there are two operating Category I facilities licensed by the NRC in the United States

2. Category II Fuel Cycle Facilities

   A. Licensed to receive, possess, use, and store special nuclear material of moderate strategic significance

   B. A Category II quantity of material is:

      (1) Less than a Category I quantity of SSNM, but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) or more than 500 grams of uranium-233, or plutonium, or in a combined quantity of more than 1,000 grams when computed by the equation,

      grams = (grams contained U-235) + 2 (grams U-233 + grams plutonium); or

DRAFT

[7] Source material – Natural uranium or thorium or depleted uranium that is not suitable for use as reactor fuel

[8] Nuclear material – Uranium, plutonium or another substance which is or may be used for extraction of nuclear energy (nuclear fuel), or a compound containing such a substance; thorium or another substance suited for conversion into nuclear fuel, or a compound containing such a substance; and spent nuclear fuel which has not been placed in final storage.

(2) Ten thousand grams or more of uranium-235 (contained in uranium enriched to 10 percent or more, but less than 20 percent in the U-235 isotope).

C. Currently, there are two NRC licensed facilities in the United States authorized to possess Category II-level special nuclear material, but these facilities do not fabricate fuel

3. Category III Fuel Cycle Facilities

A. Licensed to receive, possess, use, and store special nuclear material of low strategic significance

B. A Category III quantity of material is:

(1) Less than an amount of special nuclear material of moderate strategic significance, but more than 15 grams of uranium-235 (contained in uranium enriched to 20 percent or more in U-235 isotope) or 15 grams of uranium-233, or 15 grams of plutonium, or the combination of 15 grams when computed by the equation,

grams = (grams contained U-235) + (grams plutonium) + (grams U-233); or

(2) Less than 10,000 grams, but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more, but less than 20 percent in the U-235 isotope); or

(3) Ten thousand grams or more of uranium-235 (contained in uranium enriched above natural but less than 10 percent in the U-235 isotope)

C. Manufacture fuel assemblies for commercial nuclear reactors

D. Currently, there are four operating Category III fuel fabrication facilities licensed by the NRC in the United States

4. Category III Fuel Enrichment Facilities (Gaseous Diffusion Plants (GDPs))

A. Certified to receive, possess, use, and store source material (SM) (or natural uranium, less than 2 percent enriched) and special nuclear material (SNM)

B. Manufacture feed materials in the form of enriched uranium hexafluoride (UF_6) for commercial fuel fabricator facilities

C. Currently in the United States, there is one operating GDP and one in cold shutdown. Both are operated by the USEC, which was created as a government corporation under the Energy Act of 1992, and privatized by legislation in 1996

5. Uranium Conversion Facility (Uranium Hexafluoride Production Facility)

A. Licensed to receive, possess, use, and store source material (natural uranium)

DRAFT

B. Manufacture feed materials in the form of UF_6 for commercial fuel-enrichment facilities

C. Currently in the United States there is one UF_6 production facility licensed by the NRC.

The NRC is reviewing applications for three additional fuel cycle facilities, including a mixed oxide (plutonium-uranium) fuel fabrication facility in Savannah River, SC, which would be a Category I facility, and two gas centrifuge enrichment plants in Eunice, NM, and Piketon, OH, which would be Category III facilities.

Uranium mining and milling facilities also are part of the fuel cycle facility category. A uranium mill is a chemical plant designed to extract uranium from mined ore. The mined ore is brought to the milling facility via truck where the ore is crushed and leached. In most cases, sulfuric acid is used as the leaching agent, but alkaline leaching can also be used. The leaching agent not only extracts uranium from the ore, but also several other constituents like molybdenum, vanadium, selenium, iron, lead, and arsenic. The product produced from the mill is referred to as "yellow cake" because of its yellowish color.

Uranium is extracted from ore at uranium mills and at in situ leach facilities. The "yellow cake" generated by both processes is sent to a conversion facility for the next step in the manufacture of nuclear fuel. The uranium milling and disposal of byproduct material[9] by NRC licensees is regulated under 10 Code of Federal Regulations[10] (CFR) Part 40, Appendix A.

Conventional mills crush the pieces of ore and extract 90 to 95 percent of the uranium from the ore. Mills are typically located in areas of low population density, and they process ores from mines within about 30 miles of the mill. Most mills in the United States are in decommissioning, one is in cold shutdown mode, and one is in operation.

In situ leach (ISL) facilities are another means of extracting uranium from underground. ISL recover uranium from low-grade ores that may not be economically recoverable by other methods. In this process, a leaching agent such as oxygen with sodium carbonate is injected through wells into the ore body to dissolve the uranium. The leach solution is pumped from the formation, and ion exchange is used to separate the uranium from the solution. About 12 such ISL facilities exist in the United States.

1.1.2.2 U.S. Low-Level Radioactive Waste Disposal

Low-level waste includes items that have become contaminated with radioactive material, or have become radioactive through exposure to neutron radiation. This waste typically consists of contaminated protective shoe covers and clothing, wiping rags, mops, filters and resins, reactor water treatment residues, equipment and tools, luminous dials, catheters, swabs, injection

[9] Byproduct material – Generally, nuclear material (other than special nuclear material) that is produced or made radioactive in a nuclear reactor. Also the tailings and waste produced by extraction or concentration of uranium or thorium from an ore processed primarily for its source material content.

[10] Code of Federal Regulations (CFR) - The codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation. Each volume of the CFR is updated once each calendar year and is issued on a quarterly basis.

needles, and syringes. Also included is radioactive waste, identified as greater than Class C[11] (GTCC) low-level waste. The radioactivity can range from just above background levels found in nature to very high levels in certain cases, such as parts from inside the reactor vessel in a nuclear power plant. Low-level waste can be stored onsite by licensees until the radioactivity has decayed away and the items can be disposed of as ordinary trash, or the waste can be accumulated and shipped to a low-level waste disposal site in containers specified or approved by DOT or the NRC.

Commercial low-level waste disposal facilities must be licensed by either the NRC or an Agreement State (the Agreement State program is described later in this section), in accordance with health and safety requirements. The facilities must be designed, constructed, and operated to meet safety and environmental protection standards. The operator of the facility must also extensively characterize the site on which the facility is located and analyze how the facility will perform for at least 500 years.

Sometimes, low-level waste disposal facilities can also store chemical waste as well. In those cases, the facility is considered to be both in the Nuclear Sector and the Chemical Sector.

There are currently three low-level waste disposal facilities in the United States that accept various types of low-level waste. These facilities, located in Barnwell, SC; Hanford, WA; and Clive, UT; are situated in and are regulated by Agreement States.

1.1.2.3 U.S. High-Level Radioactive Waste Disposal

High-level radioactive wastes are the highly radioactive materials produced as a byproduct of the reactions that occur inside nuclear reactors. High-level wastes take one of three forms:

1. Irradiated nuclear fuel
2. The highly radioactive material remaining after spent fuel is reprocessed (note: reprocessing of spent fuel from commercial nuclear reactors is not performed in the United States)
3. Other highly radioactive material that the NRC, consistent with existing law, determines by rule requires permanent isolation

Because of their highly radioactive fission products, high-level waste and spent fuel must be handled and stored with care. Since the only way radioactive waste becomes radioactively harmless is through decay, the waste must be stored and finally disposed of in a manner that provides adequate protection of the public.

[11] Greater Than Class-C (GTCC): Defined in the Low-Level Waste (LLW) Policy Amendments Act of 1985 as LLW that exceeds the Class C limits in 10 CFR Part 61.55, "Licensing Requirements for Land Disposal of Radioactive Waste." This section classifies LLW as Classes A, B, or C, according to concentration of specific short- and long-lived radionuclides; this section also sets varying requirements on waste forms for disposal. Most forms of GTCC waste are generated by routine operations at nuclear power plants, fuel research facilities, manufacturers of radiopharmaceuticals and sealed sources used in medical and industrial applications, and in moisture and density gauges, and contaminated trash. GTCC waste is generally unacceptable for near-surface disposal.

The Department of Energy is preparing a license application to submit to the NRC for construction authorization for a high-level waste repository at Yucca Mountain, approximately 100 miles northwest of Las Vegas, NV. The DOE had stated that it intended to submit the license application to the NRC in December 2004, but that schedule was delayed when the US Court of Appeals ruled that the EPA standards on Yucca Mountain violated Federal laws and must be rewritten. The Nuclear Waste Policy Act of 1982, as amended, specifies that the NRC will issue a decision on the license application 3 to 4 years after receiving it from DOE. The NRC may issue a license if DOE can demonstrate that it can construct and operate the repository in compliance with NRC safety and security regulations in 10 CFR Part 63.

1.1.2.4 Spent Fuel Storage

All of the operating nuclear power reactors are storing spent fuel under NRC licenses in spent fuel pools (SFPs) located within the site's protected area.

In addition to storage in the pools, there are approximately 33 licensed independent spent fuel storage installation sites (ISFSIs) where spent fuel is stored in the United States. Twenty-five operating power plants have ISFSIs, along with two decommissioned power plant sites, four power plant sites that are in the process of decommissioning, an interim storage facility operated by DOE at the Idaho National Laboratory near Idaho Falls, Idaho, and the General Electric-Morris operation in Illinois, which is licensed for wet storage of spent fuel.

In 1990, the NRC amended its regulations to authorize storage of spent fuel at reactor sites in dry cask-storage systems approved by the NRC. Dry cask storage allows spent fuel that has already been cooled in the spent fuel pool for a minimum of 1 year to be transferred to an NRC-certified storage cask. Although the minimum storage time in the spent fuel pool is specified as one year, spent fuel eventually transferred to dry cask storage has typically been in the spent fuel pool for 5 or more years. Dry storage, which is almost completely passive, is simpler and uses fewer support systems than spent fuel pools. Dry storage is not suitable for spent fuel until the fuel has been out of the reactor for several years and the amount of heat generated by radioactive decay has been reduced, otherwise, an active cooling system would be required. The casks are typically steel cylinders that are either welded or bolted closed. The steel cylinder provides robust containment and confinement of the spent fuel. Each cylinder is surrounded by additional steel, concrete, or other material to provide radiation shielding to workers and members of the public. Some cask designs, referred to as dual-purpose canisters, can be used for both storage and transportation.

Private Fuel Storage (PFS), a consortium of electric utilities, applied to NRC for a license to store 44,000 tons of high-level waste in steel and concrete casks on the Skull Valley Band of Goshute Indians reservation in 1997. On February 21, 2006, the commissioners of the NRC issued a license to PFS to begin construction and operation of the spent fuel storage facility. Separate from the NRC actions, the Bureau of Indian Affairs must issue final approval of the lease between the company and the Skull Valley Band of Goshute Indians. Also, the Bureau of Land Management must approve a revision of the land resource management plan for Skull Valley to permit PFS to construct and operate a rail line on a right-of-way through Bureau of Land Management land to connect the PFS site and the Union Pacific Railroad main line. If all approvals are granted, PFS is still not expected to begin operating before 2007.

DRAFT

1.1.2.5 Nuclear Materials Users and Sources

Nuclear materials are in widespread use in our Nation. They provide critical capabilities in the oil and gas, electrical power, construction, and food industries; are used to treat millions of patients each year in diagnostic and therapeutic medical procedures; are used in a variety of law enforcement and military applications; and are used in many areas for technology research and development (R&D) involving academic, government, and private institutions. These materials are as diverse in geographical location as they are in functional use. The radioactive material for medical diagnostic procedures, and for research and development, may be used in many chemical and physical forms. Industrial uses principally involve encapsulated nuclear material or sealed sources. There are millions of radioactive sources in the United States, and tens of thousands of authorized users (licensees). The amount of radioactive material authorized for use by these licensees varies from one one-millionth of a curie to millions of curies (i.e., sources used in large irradiators). There is a graded regulatory approach to safety and security that is generally consistent with potential radiation risk from these materials. Oversight of regulated radioactive materials is commensurate with the level of risk to workers and the public that the materials pose under ordinary or accident conditions, when used for their intended purposes. Only a very small subset of the radioactive sources, utilized by less than 2,000 NRC and Agreement State licensees, are considered risk-significant for security reasons consistent with the International Atomic Energy Agency's (IAEA's) Code of Conduct on the Safety and Security of Radioactive Sources. Consequently, these radioactive materials in quantities of concern[12] require the implementation of additional security measures (ASMs) and increased controls to enhance their protection from theft or sabotage.

Byproduct material is radioactive material (except for special nuclear material) yielded or made radioactive by exposure to the radiation incident to the process of producing or utilizing special nuclear material, and the tailings or wastes produced by the extraction, concentration, uranium, thorium from any ore primarily for its use as source material content. Examples of byproduct material include cobalt-60, cesium-137, and iridium-192. Source material is uranium or thorium, or any combination thereof, in any physical or chemical form, or ores that contain, by weight, one-twentieth of one percent of these elements.

The Atomic Energy Act (AEA) of 1954, as amended, gives responsibility and authority for the control of special nuclear material, source material, and byproduct material to the NRC. Under the AEA, the NRC is authorized to transfer some of its authority to States on a State-specific basis. To date, 33 states, known as Agreement States, have entered into agreements with the NRC to regulate the use of byproduct material, as authorized by the AEA. The complete list of Agreement States, as of November 2005, is listed in Table 2. Agreement States issue licenses[13]

DRAFT

[12] Radioactive materials in quantities of concern are considered to be Category 1 and 2 sources, based on the definitions of Category 1 and 2 sources in the IAEA Code of Conduct on Safety and Security of Radioactive Sources (July 2003). That document states that Category 1 sources, if not safely managed or securely protected would be likely to cause permanent injury to a person who handled them, or were otherwise in contact with them, for more than a few minutes. It would probably be fatal to be close to this amount of unshielded material for a period of a few minutes to an hour. Category 2 sources, if not safely managed or securely protected, could cause permanent injury to a person who handled them, or were otherwise in contact with them, for a short time (minutes to hours). It could possibly be fatal to be close to this amount of unshielded radioactive material for a period of hours to days.

[13] License: A license issued under the regulations of Parts 30 through 36, 39, 40, or 70 of Title 10 of the Code of Federal Regulations or by an Agreement State under its equivalent regulations. Specific licenses are issued for medical, academic, and industrial uses of nuclear materials. Reactor-produced radionuclides are used extensively throughout the United States for civilian and military industrial applications; basic and applied research; the manufacture of consumer products; civil defense activities;

and regulate approximately 17,000 materials licensees, only a small fraction of whom possess radioactive materials in quantities of concern. However, even in Agreement States, the NRC maintains jurisdiction over nuclear reactors, radioactive sources used by Federal agencies, and matters regarding the common defense and security in the use of byproduct material. States have the primary responsibility and authority over naturally occurring radioactive materials not addressed in the Atomic Energy Act. The NRC issues licenses and regulates approximately 4,500 byproduct materials licensees.

Table 2: List of NRC Agreement States

Alabama	Arkansas	Arizona
California	Colorado	Florida
Georgia	Illinois	Iowa
Kansas	Kentucky	Louisiana
Maine	Maryland	Massachusetts
Mississippi	Nebraska	Nevada
New Hampshire	New Mexico	New York
North Carolina	North Dakota	Ohio
Oklahoma	Oregon	Rhode Island
South Carolina	Tennessee	Texas
Utah	Washington	Wisconsin

1.1.2.6 U.S. Nuclear Materials Transportation

Licensed radioactive materials are shipped in accordance with the hazardous materials transportation safety and security regulations of the DOT and NRC. The responsibilities of the two Agencies are generally divided as follows:

- The Department of Transportation regulates shippers and carriers of hazardous materials, including radioactive material. The DOT is responsible for such items as vehicle safety, routing, shipping papers, hazard communications, certain packaging requirements and emergency response information, and shipper/carrier training requirements.
- The NRC regulates users of radioactive material and approves the design, fabrication, use, and maintenance of shipping containers for more hazardous domestic radioactive material shipments. It also regulates the physical protection of commercial spent fuel and large quantities of radioactive material in transit against sabotage or other malicious acts.
- The exception to this is while the NRC regulates the security measures applied to commercial shipments, they do not regulate the physical protection of DOE/Civilian Radioactive Waste Management shipments. DOE regulates those shipments. The Nuclear Waste Policy Act, as amended, requires that NRC certify the packages in which

academic studies; and for medical diagnostics, treatment, and research. The regulatory programs of NRC and Agreement States are designed to ensure that licensees safely use these materials and do not endanger public health and safety nor cause damage to the environment.

DOE transports and that DOE comply with NRC's shipment pre-notification regulations. DOE via its Orders regulates all other aspects of transportation, including physical protection.

Packages of low-hazard radioactive material are shipped throughout the United States by rail, air, and sea, and over roads. These packages contain small quantities of radioactive material typically used in industry and medicine. These packages are designed to provide a safe and economical means of transporting relatively small quantities of radioactive material. The regulations prescribe limits on the maximum amounts of radioactivity that can be transported in these packages, such that doses from any accidents involving these packages will have no substantial health risks. Examples include transport of smoke detectors, exit signs, watch dials, radiopharmaceuticals, and such slightly contaminated equipment as syringes used to administer radiopharmaceuticals.

Safety standards for the more hazardous radioactive material packaging in casks are set forth in NRC regulations. Casks must be designed to withstand a series of impacts, punctures, and fire environments, and a deep-water-immersion test, thereby providing reasonable assurance that packages will withstand serious transportation accidents. An approval certificate for the design must be issued by the NRC before a cask can be used to domestically transport more hazardous radioactive material, such as spent fuel, or high-activity sources used in panoramic irradiators. The DOT, in consultation with the NRC, revalidates foreign certificates for casks used in international shipments.

The standards established in NRC regulations require that shipping containers, or casks, prevent the loss or dispersion of their radioactive contents, provide adequate shielding and heat dissipation, and prevent nuclear criticality (a self-sustaining nuclear chain reaction) under both normal and accident conditions of transport.

1.1.3 Decommissioning

Decommissioning is the safe removal of a facility from service, and reduction of residual radioactivity to a level that permits release of the property and termination of the owner's license. The NRC requires that decommissioned facilities adhere to the regulations requiring protection of the radioactive materials on site. During decommissioning, nuclear power reactors continue to store spent nuclear fuel onsite, requiring the continuation of security requirements.

1.1.4 The Human Element

There is a human element to each Nuclear Sector asset, system, network, and function. This human element requires:

- Identifying and preventing the insider threat resulting from infiltration or individual employees determined to do harm;
- Identifying, protecting, and supporting (e.g., via cross-training) employees and other persons with critical knowledge or functions; and
- Identifying and mitigating fear tactics used by terrorist agents, insider attackers, and misinformed media sources.

DRAFT

Some of the ways that this is specifically addressed in the Nuclear Sector includes: background checks for employees; extra protective measures in place to safeguard the most critical employees; and exercises and drills to physically and mentally prepare employees for potential terrorist activity.

1.1.5 The Cyber Element

[paragraph to be inserted here]

1.1.6 Interdependencies and Overlapping Relationships with Other Sectors

Many assets are dependent on multiple elements and systems to maintain functionality. In some cases, a failure in one sector will have a significant impact on the ability of another sector to perform necessary functions. This reliance on another sector for functionality of certain assets is called a dependency. If two assets are dependent on one another, then they are interdependent. It is extremely important to identify dependencies and interdependencies both at the sector and asset level in order to fully understand the consequences of a successful attack on an asset and to identify the manner in which attacks on other assets could impact an interdependent asset.

Overlaps exist where assets fit into more than one of the seventeen CI/KR sectors based on their characteristics or functions. For instance, the Hoover Dam is a key resource located in the Dams Sector, but also could be classified as an Energy Sector asset due to its hydro-electric power generation capabilities, a Transportation Sector asset due to the highway that runs over the dam, and a National Monuments and Icons Sector asset. It is important to identify overlaps at the sector level both to minimize the duplication of effort by overlapping SSAs, and to ensure that assets are not being ignored as a result of overlapping SSAs believing that other SSAs are responsible for securing a specific type of asset.

Table 3 identifies the CI/KR sectors that are interdependent or overlap with the Nuclear Sector. DHS is working with the SSAs responsible for each of the sectors identified below to enhance the security of interdependent or overlapping assets.

Table 3: Nuclear Sector Interdependencies and Overlaps With Other CI/KR Sectors

Sector (Sector-Specific Agency)	Interdependency/Overlap With the Nuclear Sector
Transportation Systems (DHS/TSA)	The Nuclear Sector overlaps with, and is dependent on, the Transportation Systems Sector in regard to the transportation of materials by land, water, and air. Modes of transportation used to ship nuclear and radiological materials in various stages of the value chain include ships, barges, trains, trucks, and airplanes. Harm to the Transportation Systems Sector has the potential to seriously hinder the movement of materials and cause cascading effects throughout the Nuclear Sector.

Table 3: Nuclear Sector Interdependencies and Overlaps With Other CI/KR Sectors

Sector (Sector-Specific Agency)	Interdependency/Overlap With the Nuclear Sector
Energy (DOE)	The Nuclear Sector overlaps with the Energy Sector as a result of its production of electricity. The Energy Sector has primary responsibility for electric power. Additionally, much like most other sectors, the Nuclear Sector is dependent on the Energy Sector for power. An interruption to the power supply would directly affect nuclear facilities located in the region serviced by the downed electric grid.
Emergency Services (DHS/CNPPD)	Due to its uniquely hazardous characteristics, the Nuclear Sector has a number of entities specifically designed to provide emergency response services to incidents. Examples of these Nuclear Sector-specific emergency services include State emergency response commissions and local emergency planning committees; the U.S. National Response Team; the National Response Center; USCG strike teams; and EPA regional response teams.
Public Health/ Healthcare (HHS)	The Public Health/Healthcare Sector is dependent on the Nuclear Sector for many items, including pharmaceuticals, and diagnostic substances. A successful attack on the Nuclear Sector potentially could have a cascading impact on the Public Health/Healthcare Sector.
Information Technology (DHS)	Like all other sectors, the Nuclear Sector is dependent on the Information Technology Sector. Many of the Sector facilities rely heavily on information technology to manage day-to-day operations at their facilities, including facility security. Additionally, information technology is used by DHS, the Nuclear SCC, the NRC, industry associations, and others to disseminate security and threat information.
Telecommunications (DHS)	Like all other sectors, the Nuclear Sector depends on the Telecommunications Sector for much of its communications capability.
Chemical (DHS/CNPPD)	The Nuclear and Chemical Sectors are interdependent in that the principal hazard to public health and safety during an accident at a fuel cycle facility would be from the release of chemicals.
CI/KR in close physical proximity to Nuclear Sector assets	If an attack occurs on CI/KR in close proximity to Nuclear Sector assets, that attack can impact the Nuclear Sector assets in the area. Also, attacks on Nuclear Sector assets can potentially impact other CI/KR in close proximity. The latter is reviewed through Comprehensive Reviews and RAMCAP (both to be discussed later in more detail), as well as during the licensing process for commercial nuclear power plants.

In addition to the dependencies and interdependencies identified above, international interdependencies must be taken into account in order to accurately assess sector-wide risks and vulnerabilities. Unfortunately, there currently is no established method to identify international interdependencies. DHS will work with private sector members of the Nuclear Sector, as well as the Commerce Department in partnership with the Department of State

DRAFT

(DOS) and industry trade associations to attempt to determine a method for identifying Nuclear Sector international interdependencies. Once international interdependencies have been established, CNPPD as the SSA will work with the rest of DHS to gather and protect information on the foreign infrastructure on which the Nuclear Sector in the United States depends. By developing an international relationship, the Nuclear Sector can begin to promote best practices and share security information with other countries through international/multinational organizations.

1.2 Security Partners

1.2.1 Department of Homeland Security

The Department of Homeland Security is the sector-specific agency responsible for this sector. DHS works with the NRC, consistent with paragraph 29 of HSPD-7. CNPPD represents DHS with respect to the other stakeholders in this sector, and will collaborate with the private sector consistent with paragraph 25 of HSPD-7. It works closely with the Risk Management Division (RMD) and the Infrastructure Partnerships Division (IPD) within DHS to execute this responsibility.

DHS has numerous responsibilities in its role as the focal point for cyberspace security and for leading, integrating, and coordinating the overall national effort to enhance CI/KR protection. Some of the responsibilities that directly pertain to the Nuclear Sector are:

- Coordinating, facilitating, and supporting the overall process for building security partnerships and leveraging sector-specific security expertise, relationships, and resources across CI/KR sectors, including oversight and support of the sector partnership model
- Cooperating with State, local, and tribal security partners and collaborating with the Department of State to reach out to foreign countries and international organizations to strengthen the protection of U.S. CI/KR
- Facilitating the sharing of CI/KR protection best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions
- Sponsoring CI/KR protection-related R&D, demonstration projects, and pilot programs
- Promoting national-level CI/KR protection education, training, and awareness through State, local, tribal, and private sector partners

Other organizations within DHS with key involvement in the Nuclear Sector include the Federal Emergency Management Agency (FEMA), the Science and Technology Directorate (S&T), the Transportation Security Administration (TSA), United States Coast Guard (USCG) and the Domestic Nuclear Detection Office (DNDO).

1.2.2 Sector-Specific Agency

As the SSA, CNPPD carries multiple responsibilities such as implementing the NIPP sector partnership model and the risk management framework. Listed below are some additional SSA responsibilities for the sector.

DRAFT

- ❑ Identify, prioritize, and coordinate the protection of sector CI/KR to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them
- ❑ Collaborate with all security partners including facilitating information sharing and building security partnerships
- ❑ Conduct or facilitate vulnerability assessments of the sector
- ❑ *Measure and report on progress of core and sector-specific metrics*

1.2.3 Nuclear Regulatory Commission

For over 3 decades, the NRC has regulated the civilian nuclear industry to ensure the necessary protection of (1) commercial nuclear reactors for generating electric power and nonpower nuclear reactors used for research and testing; (2) nuclear materials in medicine, industrial, and academic settings and fuel cycle facilities; and (3) the transportation, storage, and disposal of nuclear materials and waste. Since the terrorist attacks in 2001, the NRC has enhanced security of nuclear facilities[14] and materials as part of the security-safety-emergency preparedness triad essential for public safety.

The NRC exchanges technical information and operational data with a variety of industry groups and standards organizations. These exchanges include participating in standards committees or sharing other publicly available documents with such organizations as the NEI and the Institute of Nuclear Power Operators (INPO). NEI is the policy organization of the nuclear energy and technology industry that promotes the beneficial uses of nuclear energy and technology in the United States and around the world. With member participation, NEI develops policy on key legislative and regulatory issues affecting the industry.

Additionally, NRC works with NEI's Cyber Security Task Force to address rising cyber security issues at nuclear power plants and develop guidance for future cyber security initiatives for the nuclear industry.

As the regulatory agency responsible for safety and security for this sector, the NRC has developed a strategic objective that guides the NRC's allocation of resources. The objective, defined in the NRC FY 2004-2009 Strategic Plan, is to "enable the use and management of radioactive materials and nuclear fuels for beneficial civilian purposes in a manner that protects public health and safety and the environment, promotes the security of our Nation, and provides for regulatory actions which are effective, efficient, realistic, and timely." To this end, there are five strategic goals that support this objective:

1. Safety—Ensure protection of public health and safety and the environment
2. Security—Ensure the secure use and management of radioactive materials
3. Openness—Ensure openness in our regulatory process

[14] Nuclear facilities - A term that includes all facilities that are part of the nuclear sector, such as: commercial nuclear power plants; research and test reactors; nuclear fuel cycle facilities; radioactive waste management facilities; deactivated nuclear facilities; facilities housing radioactive materials; and radioactive source production and distribution facilities.

4. Effectiveness—Ensure that NRC actions are effective, efficient, realistic, and timely

5. Management—Ensure excellence in agency management to carry out the NRC's strategic objective.

The NRC is also revising its oversight program for nuclear power reactors and nuclear materials facilities to enhance the use of risk information to guide assessments of licensee performance. Among other components of this program, the NRC recently modified its physical protection oversight process to accommodate new security requirements imposed on reactor licensees since September 11, 2001. In February 2004, the NRC issued new inspection procedures for physical protection and security, and in January 2005 issued a new physical protection significance determination process (PPSDP). The PPSDP categorizes inspection findings into four bands, green (very low significance), white (low to moderate significance), yellow (substantial significance), and red (high significance). An action matrix for security and associated assessment process has been developed and has been approved by the NRC for use. Although information specific to individual plants will be available to the associated licensee, State, and Federal agencies, it will not be available to the general public.

For the purposes of this SSP, attention will be focused on the security goal above, and the manner in which it relates to the protection of the critical infrastructure in this sector. The following performance measures and strategic outcome are consistent with and support the security goal.

NRC nuclear security performance measures, which can be found in the NRC's FY 2005 Performance and Accountability Report, include:

- Number of identified losses or thefts of risk-significant radioactive materials
- Number of security events and incidents that exceed the abnormal occurrence criteria
- Number of significant unauthorized disclosures of classified and/or Safeguards Information

The NRC strategic outcome for security is that there are no instances where licensed radioactive materials are used domestically in a manner hostile to the security of the United States.

In order to measure the success of the performance measures and strategic outcome with regard to critical infrastructure protection, the NRC collects and assesses data regarding security involving licensed facilities and radioactive materials. These reports are tracked in databases maintained by the NRC. The NRC reports annually to the Congress and the Administration on its performance relative to strategic and performance measures. In addition, the NRC reports annually to the Congress on abnormal occurrences, including security incidents that satisfy the criteria. The criteria were stated in an NRC policy statement published in the *Federal Register* (FR) on December 19, 1996 (61 FR 67072).

1.2.3.1 Advisory Committees and Licensing Board

The NRC has several advisory committees to assist it in its regulatory responsibilities. The Advisory Committee on Reactor Safeguards (ACRS) has statutory responsibilities as described in the AEA, as amended. The ACRS conducts independent reviews and advises the NRC's

DRAFT

Commission, which consists of five commissioners and is the head of the NRC, about technical and policy issues concerning the licensing and operation of production and utilization facilities, and related safety issues, the adequacy of proposed reactor safety standards, and the licensing of evolutionary and passive plant designs, and other matters referred to it by the Commission.

The Advisory Committee on Nuclear Waste (ACNW) conducts independent reviews and reports to and advises the Commission on technical and policy issues related primarily to nuclear waste facilities. This includes activities related to transportation, storage, and disposal of high-level and low-level radioactive waste, including the interim storage of spent nuclear fuel; decommissioning; application of risk-informed, performance-based regulations; and evaluation of licensing documents, rules, regulatory guidance, and other issues as requested by the Commission.

The Advisory Committee on the Medical Uses of Isotopes (ACMUI) advises the NRC on policy and technical issues arising from regulation of the medical uses of radioactive material in diagnosis and therapy. The ACMUI provides input on changes to NRC medical regulations and guidance; evaluates certain nonroutine uses of radioactive material; provides technical assistance in licensing, inspection, and enforcement cases; and brings key issues to the attention of the Commission for appropriate action.

The Atomic Safety and Licensing Board Panel (ASLBP) conducts adjudicatory hearings for the Commission and performs such other functions as the Commission authorizes.

1.2.3.2 NRC Licensees

The NRC issues licenses to private sector entities and governmental agencies in the nuclear subsectors identified in Section 1.1. The NRC oversees its licensees from its headquarters offices, four regional offices, and through onsite inspectors at power reactors and certain fuel cycle facilities. The NRC carries out its regulatory mission through five main components: (1) developing regulations, orders, and guidance; (2) licensing or certifying applicants to use nuclear materials or operate specific types of nuclear facilities; (3) overseeing licensee operations and facilities to ensure that licensees comply with safety and security 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 NRC decisions, and obtaining independent reviews to support NRC regulatory decisions.

1.2.4 Other Federal Agencies and Departments

Along with DHS and the NRC, cooperative interagency activities are carried out among DOE, DOT, Health and Human Services (HHS), Department of Justice (DOJ)/FBI, Department of State, EPA, the Food and Drug Administration (FDA), Occupational Safety and Health Administration (OSHA), the intelligence community, and DOD. The NRC coordinates closely with other Federal agencies and departments by producing joint reports, participating in task forces and interagency committees to share information about issues of mutual importance, and complying with formal cooperative agreements. For example, DHS and the NRC work closely with intelligence-gathering agencies to identify potential physical and cyber threats to nuclear facilities. DOT and DOE have a special relationship with the NRC, due to the shared oversight responsibility for the transportation of radioactive material, as discussed previously.

DRAFT

Federal agencies and departments will support implementation of the Nuclear SSP and are responsible for identification, prioritization, assessment, remediation, and enhancing protection of CI/KR under their control. They will also assist in assessing risk, prioritizing CI/KR, and collaborating with sector security partners to share security-related information as appropriate.

1.2.5 Agreement States

Section 274b of the AEA allows the Commission to relinquish its regulatory authority over certain materials and certain activities in a State if three conditions are met. First, the State must have laws, regulations, and safety standards compatible with those of the NRC. Second, the State must have a regulatory program that provides a comparable degree of protection to the public health and safety as does the NRC program. Third, the Governor, on behalf of the State, must enter into a formal agreement with the NRC to assume regulatory responsibility over the materials. Note that under the agreement, the State does not enforce Federal requirements on behalf of the NRC; rather the State regulates the materials under its own authority. Currently, 33 States have Section 274b Agreements, and two additional States have announced their intention to enter into agreements.

Under 274b Agreements, the NRC interacts frequently with the States on matters of licensing, inspection, enforcement, incident response, training, and coordination of rule making. The NRC provides technical assistance, primarily to Agreement States, and sponsors conferences and special workshops on topics of interest when needed. Agreement States report significant incidents involving materials to the NRC Operations Center. More detailed event descriptions are later entered into an events database. The NRC maintains Office of Management and Budget clearances for the needed information collections.

The AEA requires the NRC to retain regulatory authority over all nuclear reactors and special nuclear material in quantities sufficient to form a critical mass, however possessed or used. The NRC also retains authority over the export of materials from and import of materials into the United States, and matters related to common defense and security. The AEA also requires the NRC to periodically review the performance of a State under its Section 274b Agreement.

1.2.6 Other States, Indian Tribes, and Related Organizations

The NRC shares safety, security, and emergency information with the States, tribal governments, licensees, and stakeholder organizations. The NRC disseminates nuclear safety information of interest to stakeholder organizations, including the Agreement States; the Conference of Radiation Control Program Directors (CRCPD), Inc; the Organization of Agreement States (OAS); the National Governors' Association; the National Association of Regulatory Utility Commissioners; and the National Congress of American Indians. Licensees communicate information on the transport of spent reactor fuel and radioactive waste to NRC and designated representatives of the States (either agreement or non-agreement). Both the NRC and the States seek public comment for significant actions. Stakeholder organizations meet publicly with the NRC to present information and concerns. State government, local government, and stakeholder organizations also communicate through established channels with the other Federal agencies active in the sector.

For events at nuclear reactors and large fuel cycle facilities, the licensee, NRC, and affected State and local government entities interact in accordance with established and practiced

DRAFT

emergency response plans. Event status information, recommended actions for public protection, and the status of implemented recommendations are shared via dedicated communications links and protocols.

1.2.7 Common Defense and Security

Since September 11, 2001, the NRC and licensees have increased their attention on the possibility of malevolent acts at nuclear facilities or malevolent use of radioactive material. The NRC has moved to protect the common defense and security of the United States by requiring additional security measures by licensees appropriate for the current threat environment. This is a responsibility that NRC is not permitted to transfer to the States; however, the AEA in section 274i permits the NRC to enter into agreements under which the States may inspect State licensees on behalf of the NRC. The NRC is developing 274i Agreements that allow interested Agreement States to inspect the Agreement State licensee implementation of additional security measures and orders issued under the NRC's common defense and security authority. Licensees have responded to the September 11, 2001 threat by implementing additional security enhancements at their facilities that add to the already robust nature of protection provided. Changes include physical, process, and personnel improvements.

1.2.8 International Community

The NRC works with such international organizations as the Organization for Economic Cooperation and Development's Nuclear Energy Agency (NEA), the International Atomic Energy Agency (IAEA), and the International Nuclear Regulators Association to help improve nuclear safety worldwide. The NRC provides for bilateral information exchange and cooperation on nuclear safety through letters of agreement with its counterpart foreign national regulatory authorities, ensuring prompt notification of safety problems that warrant action or investigation. Additionally, more than 60 joint international safety research agreements with other countries enable the sharing of technical information, funding, technical support, and the results of joint research projects and programs. To improve nuclear safety regulation of Soviet-designed reactors, the NRC exchanges safety information with the foreign regulatory counterparts through workshops, peer review of regulatory documents, working group meetings, and technical information and specialist exchanges.

The NRC also issues import and export licenses for nuclear facilities, major components, material, and related commodities, and assists in the development of legal instruments to address vital issues related to nuclear safety and security. Interagency bilateral physical protection visits are conducted to ensure the adequacy of protection of U.S.-origin materials. The United States Government has nuclear trade treaties in place with some two dozen countries, Taiwan, and the 25-nation European Union. Pursuant to these nuclear trade treaties, the United States and these entities agree that nuclear trade is for nonmilitary purposes. The U.S. Government has actively supported the IAEA effort to develop an international code of conduct on the safety and security of radioactive sources. The goal of this activity, and the associated IAEA Technical Document (TECDOC) 1344, Categorization of Radioactive Sources, is to create a harmonized global system of controls that focuses on sources of highest risk.

The NRC regularly exchanges classified or Safeguards Information with a select group of countries regarding vulnerabilities, mitigation strategies, and security improvements. These exchanges ensure that U.S. security enhancements are better understood and, where needed, in harmony with foreign government activities.

DRAFT

1.2.9 Owner/Operators, Industry Groups, Standards Organizations, and Professional Societies

All U.S. commercial nuclear power plants maintain membership in INPO. INPO provides oversight of the industry to enhance nuclear plant safety and reliability primarily through the cornerstone programs of on-site evaluations of each nuclear plant, training and accreditation, events analysis and information exchange, and assistance. The Atlanta Center of the World Association of Nuclear Operators (WANO) is co-located with INPO. WANO, formed by the international nuclear community, promotes worldwide improvements in the quality of nuclear plant operations, and the Atlanta Center is one its five world-wide regional centers. INPO provides operational support and facilities for the Atlanta Center and represents the U.S. nuclear utilities' membership in WANO.

The industry's recognition that all nuclear utilities are affected by the action of any one utility motivated its commitment to and support of INPO. Each individual member is responsible for the safe operation of its nuclear electric generating plant(s). The NRC has statutory responsibility for overseeing its licensees and verifying that each licensee operates its facility in compliance with Federal regulations. Compliance with regulations alone, however, does not necessarily result in the best possible performance. INPO's role is to promote excellence in the operation of its members' nuclear power plants.

All U.S commercial nuclear power plants maintain membership in the Nuclear Energy Institute (NEI) as do many material licensees. NEI provides the political and policy interface for the industry as well as representing the various segments of the nuclear industry in a regulatory sense for generic issues with the NRC. Working groups and task forces organized through NEI provide information exchange and establish guidelines for performance on topics ranging from security to fire protection. The NEI and the industry established the Security Working Group (SWG) to address industry security issues. The SWG is comprised of industry security managers and executives and meets frequently to coordinate and optimize industry security efforts. The SWG provides the means for the industry to strategically approach improvements to the industry's security posture.

Each nuclear utility has established a Safety Review Committee that provides additional independent oversight of the nuclear power plants. Reporting to the senior management of the utility, these committees:

- Independently review activities to provide additional assurance the units are operated and maintained in accordance with the Operating License and applicable regulations that address nuclear safety.

- Provide independent advice and counsel on the broad aspects of nuclear safety and operational performance.

Technical information is exchanged among other industry stakeholders through participation in organizations and standards committees such as the American National Standards Institute/Health Physics Society, American Concrete Institute, American Society of Civil Engineers, American Society of Mechanical Engineers (ASME), American Nuclear Society, Institute of Nuclear Materials Management, American Society for Nondestructive Testing, Electrical Power Research Institute (EPRI), and the Society for Nuclear Medicine.

DRAFT

Other industry groups represent manufacturers and distributors of radioactive materials, including those used in diagnostic nuclear medicine, medical therapy, life science and biomedical research, nondestructive testing, and irradiation of food and medical products. Groups that have been active with the NRC and other relevant agencies in the exchange of information in the process of rulemaking and policy development include the Council on Radionuclides and Radiopharmaceuticals and the Society of Nuclear Medicine.

The government has been pleased overall with the outreach that has occurred between them and the private sector. Some areas of particular strength have been working with the commercial nuclear power plants and the Research and Test Reactor (RTR) community. Still, CNPPD would like to be able to grow further its working relationships with other Nuclear subsectors, and will work to interact more with these groups.

1.2.10 Academia, Research Centers, and Think Tanks

[paragraph to be inserted here]

1.2.11 Organizations with Capabilities to Respond to a Nuclear or Radiological Emergency

Response to a nuclear or radiological emergency involves a wide variety of organizations, some of which are detailed below. The Nuclear/Radiological Incident Annex of the National Response Plan (NRP) provides an organized and integrated capability for a timely, coordinated response by Federal agencies to terrorist and other incidents involving nuclear or radioactive materials. Objective #8.1, explained in section 1.3.1.3, addresses making any appropriate revisions to the Nuclear/Radiological Incident Annex of the NRP.

CNPPD, working with the rest of DHS, other Federal agencies, and additional Nuclear Sector stakeholders, ensures seamless linkage between the NIPP and Nuclear SSP steady-state protection and incident management activities. This linkage includes the following:

- Increasing protective levels to correlate with the threat level communicated through the Homeland Security Alert System (HSAS), or in accordance with sector-specific warnings using the NIPP and Nuclear SSP information-sharing networks;
- Use the NIPP and Nuclear SSP information-sharing networks and risk management framework to review and establish national priorities for Nuclear Sector protection; facilitate communication between security partners; and inform the NRP processes regarding priorities for response, recovery and restoration of Nuclear Sector assets, systems, networks, and functions on a national scale and within the incident area; and
- Fulfill roles and responsibilities as defined in the NRP for incident management activities.

1.2.11.1 DOE National Emergency Response Assets

In the event of a nuclear weapons incident or radiological disaster, DOE maintains a response capability through the Nuclear Weapons Incident Response Program. This program supports "first responder teams" of highly specialized scientists and technical personnel from the Department's National Nuclear Security Administration (NNSA) sites who are deployed across the nation to address immediate threats from nuclear materials. These teams work with DHS

DRAFT

and the FBI, making available the Department of Energy's nuclear expertise in response to suspected nuclear emergencies in the U.S. and around the world.

When the need arises, DOE/NNSA is prepared to respond immediately to any type of radiological accident or incident, regardless of location, with seven unique radiological emergency response assets. These assets include the Aerial Measuring System (AMS), the National Atmospheric Release Advisory Capability (NARAC), the Accident Response Group (ARG), the Federal Radiological Monitoring and Assessment Center (FRMAC), the Nuclear Emergency Support Team (NEST), the Radiological Assistance Program (RAP), and the Radiation Emergency Assistance Center/Training Site (REAC/TS). Each asset handles certain aspects of the radiological emergency and performs a comprehensive and rapid integrated response. Capabilities are outlined below:

- AMS detects, measures, and tracks radioactive releases after an emergency to determine contamination levels using both fixed and rotary wing aviation assets.
- NARAC develops predictive plumes generated by sophisticated computer models.
- ARG is deployed to manage or support the successful resolution of a U.S. nuclear weapons accident anywhere in the world.
- FRMAC coordinates Federal emergency radiological monitoring and assessment activities with those of State and local agencies.
- REAC/TS provides treatment and medical consultation for injuries resulting from radiation exposure and contamination as well as a training venue.
- RAP is usually DOE/NNSA first responder for assessing the emergency situation and deciding what further steps should be taken to minimize the hazards of a radiological emergency.
- NEST provides the Nation's specialized technical expertise to the DOD or the FBI in resolving nuclear/radiological terrorist incidents.

1.2.11.2 FBI Emergency Response Assets

The FBI has various resources that, depending on the type of incident within the Nuclear Sector, may be important during the response phase. For instance, each FBI field division has a Crisis Management Coordinator, a Weapons of Mass Destruction Coordinator, SWAT Team(s), crisis negotiators, behavioral specialists, technical personnel, support personnel, and command and control personnel. There are resources at the FBI Critical Incident Response Group (CIRG) at Quantico, Virginia, including a Hazardous Devices Response Unit, Bomb Data Center, Hostage Rescue Team, Command Post Specialists, crisis negotiators, behavioral specialists, aviation support (fixed wing/helo), and SWAT Team advisors. The FBI Laboratory Division supports response to incidents utilizing its Hazardous Materials Response Unit (HMRU), Evidence Response Team Unit, and Scientific Analysis Section. The Information Resources Division has a Crisis Response Team (communications/technical) and data processing support.

1.2.11.3 DOD Emergency Response Assets

DOD has a number of Weapons of Mass Destruction Civil Support Teams (WMD-CST) that are able to rapidly deploy, and assist local first responders in determining the nature of an attack, provide medical and technical advice, and pave the way for the identification and arrival of

DRAFT

follow-on State and Federal military response assets. The mission of WMD-CSTs is to assess a suspected nuclear, biological, chemical, or radiological event in support of the local incident commander, advise civilian responders regarding appropriate courses of action; and facilitate requests for assistance to expedite arrival of additional State and Federal assets to help save lives, prevent human suffering and mitigate significant property damage. WMD-CSTs could be called upon in the event of some incidents involving the Nuclear Sector.

1.2.11.4 Interagency Emergency Response Assets

The Domestic Emergency Support Team (DEST) is a specialized, rapidly deployable, interagency team composed of subject matter experts from the FBI, FEMA, DOD, DOE, HHS, and EPA. It provides guidance to the FBI Special Agent in Charge (SAC) concerning WMD threats and actual incidents, and has limited operational capacity.

1.3 Sector Security Goals

Sector security goals state the comprehensive protective posture that the government and infrastructure owners and operators are working together to achieve for the sector and will help lead to a steady-state of protection. These goals reflect the overall risk management outcomes that owners/operators and government leaders seek. Once developed, these goals will inform the objectives sought and activities performed during the implementation of the remaining steps of the Risk Management Framework.

These goals were developed utilizing the full spectrum of protective activities (i.e., awareness, prevention, protection, response, and recovery). These five areas correspond to five of the goals from the DHS Strategic Plan. Those five terms are defined in the DHS Strategic Plan as:

- Awareness – Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.
- Prevention – Detect, deter, and mitigate threats to the homeland.
- Protection – Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.
- Response – Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies
- Recovery – Lead national, State, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

The successful efforts taken to meet the goals and objectives in the sector while addressing awareness, prevention, protection, response, and recovery will help the Nuclear Sector achieve a long-term security posture.

1.3.1 Elements and Characteristics of Sector Security Goals

1.3.1.1 Sector Vision

The Nuclear Sector Vision Statement, which concisely describes the ideal protective posture for the Sector, is:

DRAFT

The Nuclear Reactors, Materials, and Waste Sector[15] will support national security, public health and safety, public confidence and economic stability by enhancing, where necessary and reasonably achievable, its existing high level of readiness to promote the security of the Nuclear Sector; and to lead by example to improve the nation's overall critical infrastructure readiness.

1.3.1.2 Sector Security Goals

The Nuclear Sector Vision Statement helped in the development of the Sector Security Goals, which are grouped into the five DHS Strategic Goals that comprise the spectrum of protective activities:

- Awareness
  - Goal #1[16] - Establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities. (Office of Primary Responsibility (OPR): NRC, DHS)
  - Goal #2 - Determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector. (OPR: RMD)
- Prevention
  - Goal #3 - Prevent nuclear and radioactive material from being used for malevolent purposes. (OPR: DNDO)
  - Goal #4 - Coordinate with Federal, State, and local Law Enforcement Agencies to develop tactics to deter, detect and prevent terrorist attacks on fixed nuclear facilities. (OPR: RMD)
- Protection, Recovery, and Response
  - Goal #5 – Protect the cyber assets of the nuclear sector from being exploited. (OPR: CNPPD, NRC, private sector)
  - Goal #6 – Utilize R&D to better protect the Nuclear Sector from future threats. (OPR: DHS).
  - Goal #7 – Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements. (OPR: CNPPD)
  - Goal #8 – Enhance the ability of the Federal, State, Territorial, tribal, local, and private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents. (OPR: CNPPD)

DRAFT

[15] The sector does not include DOD and DOE nuclear facilities associated with defense related activity. However, the sector does include DOE Research and Test Reactors.

[16] The numbering of the goals is not to identify priorities, but is for identification purposes only.

1.3.1.3 Sector Security Objectives

Each Sector Security Goal has objectives associated with it. The objectives are specific activities that will be taken in order to achieve progress towards accomplishing the goals. The objectives also help identify how to measure the progress in achieving the goal (which will be discussed in further detail in Chapter 7).

On a goal-by-goal basis, the objectives for the goals are:

1. Establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities.
   - Define, identify and maintain the key points of contacts (POCs) having security and emergency response responsibilities for the Nuclear Sector.
   - Communicate clear, timely, and comprehensive threat and intelligence information as appropriate.
   - Increase public awareness of the consequences and proper actions following a release of radioactive material.
   - Increase public awareness of protective measures in place in the Nuclear Sector, at a level of detail that would help deter rather than encourage or help enable, a terrorist attack.
   - Share lessons-learned from previous nuclear and radiological events within the sector.
2. Determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector.
   - Identify Nuclear Sector dependencies and interdependencies in order to fully understand and plan for the consequences of an interruption of service from another critical infrastructure or key resource as well as consequences to other sectors.
3. Prevent nuclear and radioactive material from being used for malevolent purposes.
   - Improve capability to detect unauthorized nuclear and other radioactive materials at key U.S. entry points where these materials either enter the U.S. or pass through before being transported to other countries.
   - Improve capability to detect unauthorized shipments of nuclear and other radioactive materials within the U.S.
   - Improve security for legitimate shipments of nuclear and radioactive materials physically transported in the United States, using a graded approach.[17]

DRAFT

[17] This objective includes developing a program of interaction among the Department of State (DOS), NRC, DOT, DOE, and DHS (CNPPD/RMD/Domestic Nuclear Detection Office [DNDO]/US Coast Guard [USCG]), which considers private sector input, to clearly define the roles and responsibilities associated with tracking legitimate shipments of nuclear and radioactive material into or through this country, with international support and consensus, by identifying gaps and recommending enhancements to close gaps.

- Improve security and tracking of all risk-significant (Category 1 and 2) sources that are in legitimate use within the U.S.
- Through grant programs, improve capabilities of the private sector to better secure their risk-significant (Category 1 and 2) sources. [placeholder objective]
- Through grant programs, locate and recover risk-significant (Category 1 and 2) sources that are declared excess and unwanted. [placeholder objective]

4. Coordinate with Federal, State, and local Law Enforcement Agencies to develop tactics to deter, detect and prevent terrorist attacks on fixed nuclear facilities and sites using risk-significant radioactive sources.
   - Develop Buffer Zone Protection Plans (BZPPs) for all commercial nuclear power reactors (and associated spent fuel facilities) and fuel cycle facilities by December 2007.
   - Work with local authorities and regulators to identify licensees within the jurisdiction and provide assistance in assessing licensees' security of risk-significant sources and in developing plans to respond to terrorist events at licensees' sites.
   - Increase local authorities' awareness of consequences of malicious use of risk-significant (Category 1 and 2) sources. [placeholder objective]
5. Protect the cyber assets of the nuclear sector from being exploited.
   - Implement the NRC recommended cyber security programs at all the commercial nuclear power plants.
   - Ensure that the industry maintains awareness of the latest cyber security measures developed or recommended by DHS/National Cyber Security Division (NCSD) and by other government-industry bodies concerned with cyber security.
6. Utilize R&D to better protect the Nuclear Sector from future threats.
   - Create an annual report summarizing the R&D planning process results.
7. Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements.
   - Complete CRs of existing commercial nuclear power reactors by December 2007.
   - Complete assistance visits to selected Research and Test Reactors (RTRs) by the end of December 2006.
   - Evaluate other subsectors within the sector to determine which warrant assessments, prioritize the order of assessments, and complete assessments in the chosen areas by December 2010.
   - Ensure that each facility in a nuclear subsector, which is above a certain risk-threshold, has an emergency response plan commensurate with the level of risk associated with the facility.
8. Enhance the ability of the Federal, State, Territorial, tribal, local, and private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents.

DRAFT

- Review and revise, as appropriate, the Nuclear/Radiological Incident Annex to the National Response Plan to better delineate the roles and responsibilities of Federal departments and agencies in preventing, preparing for, responding to and recovering from nuclear or radiological incidents.
- Incorporate emergency preparedness (EP)-security-based scenarios into the Emergency Preparedness drill and exercise programs for commercial nuclear power facilities.
- Incorporate prompt notification technologies such as Automated Ring Down circuits between the DHS NICC and all Cat 1 and NPP's within the sector.

1.3.1.4 Cross-sector Elements of Goals

Organizations are in place for both industry and government to coordinate between sectors. The Partnership for Critical Infrastructure Security is utilized by industry to work with other CI/KR sectors, in an effort for all sectors to improve their protective posture. For government, the NIPP Federal Senior Leadership Council brings together all the Sector-Specific Agencies (SSAs). These coordination activities are described further in the NIPP.

While the goals and objectives listed above are for the Nuclear Sector, some of the goals and objectives also benefit other sectors, and may require coordination with those other sectors. For instance, the CRs in one of goal #6's objectives also involves interaction with the Emergency Services Sector, as the two sectors work together to improve the emergency response to a Nuclear Sector asset. Goal #2 specifically addresses determining the various dependencies and interdependencies associated with any CI/KR sector. Goal #5 addressing cyber protection has a tie with the Information Technology sector. Tracking and securing shipments of nuclear and radiological material, discussed in some of goal #3's objectives, also involves the Transportation Sector.

1.3.2 Process to Establish Sector Security Goals

1.3.2.1 Initial Establishment of Goals

In order to help develop sector security goals and draft this Sector-Specific Plan, a Nuclear SSP Working Group was formed, with representation from a wide spectrum of private and public sector entities that is similar in nature to the combined representation on the GCC and NSCC. This Working Group met a number of times to develop and then revise the goals. The GCC and NSCC will have an opportunity to review and approve the goals, and an even larger cross-section of the sector will have a chance to comment on the goals during the SSP's review process.

The GCC and the NSCC led the way with developing a vision for the sector that the Nuclear SSP Working Group kept in mind as it developed the goals. The Working Group adopted the five goals previously mentioned from the DHS Strategic Plan to provide an overall structure for the Nuclear Sector Security Goals. The GCC and the NSCC will approve the Nuclear Sector goals, as well as this document as a whole, prior to final publication of the NSSP.

DRAFT

1.3.2.2 Revisions to Goals and Objectives

The SSA, in coordination with the GCC and NSCC, will reexamine the goals and objectives on an annual basis, or more frequently if necessary, considering changes in the sector's security posture, to determine if any modifications should be made.

1.3.3 Cross-Sector Initiatives

Due to the dependencies and interdependencies between the Nuclear Sector and the other CI/KR sectors, some initiatives in order to achieve the these goals and objectives will need to cut across sectors. For instance, Goal #5 addressing cyber security has connections to the IT Sector for which the DHS/National Cyber Security Division (NCSD) is the SSA. Goal #8 and other goals and objectives that address emergency response will benefit from interaction with the Emergency Services Sector. CNPPD is the SSA for both the Nuclear Sector and the Emergency Services Sector. Goal #2 continues the work in further understanding other dependencies and interdependencies that the Nuclear Sector has.

Some goals and objectives can benefit other sectors as well. For instance, the Automated Ring Down technologies discussed in one of Goal #8's objectives will probably involve DHS developing a prompt notification system using Automated Ring Down technologies for all 17 CI/KR, not just the Nuclear Sector's critical facilities. By doing so, DHS can ensure that prompt notification between a critical asset under attack and the NICC will be as fast and simple as possible. Upon receipt of the call the DHS can step through a preplanned set of calls that will be able to engage the relevant response features of the National Response Plan. In addition, by using the National Asset Database (NADB) and the same Automated Ring Down lines, the DHS can notify all other impacted CI/KR within some relevant geographical area. This will inform the other elements of the CI/KR community in the vicinity of the affected resource within a very short time that they may need to be on guard.

1.4 Value Proposition

There is a strong incentive for the private sector to participate in information sharing with DHS/SSA. The following are some reasons the private sector should consider information sharing an advantage rather than a liability:

- Proprietary or business sensitive infrastructure information can be shared with governmental entities that share the private sector's commitment to a more secure homeland.
- Information sharing will result in better identification of risks and vulnerabilities, which will help industry partner with others in protecting key assets.
- Industry is helping to safeguard and prevent disruption to the American economy and way of life.
- Private industry is demonstrating good corporate citizenship that may save lives and protect communities.
- The Nuclear industry recognizes that a successful attack on a nuclear facility would be devastating to the industry and therefore, it is in their best interest to detect and deter a terrorist attack before it occurs or if one should occur, to be able to successfully defend their facilities against it.

DRAFT

Some of the ways that information can be protected includes the Protected Critical Infrastructure Information (PCII) Program, categorizing information as Safeguards Information (SGI), and classifying information. Section 2.5 contains more about protecting information.

1.5 Challenges

As the sector-specific agency for this diverse sector, DHS/CNPPD recognizes the importance and challenges associated with growing communications links between itself; Federal, State, and local government; and private sector stakeholders. Establishing the GCC and the NSCC is one way that the communication links are established.

The commercial nuclear power plants have a very structured protocol for communications with the NRC, State and local organizations. Procedures and policies establishing these protocols have been tested over time and remain in place due to their effectiveness. With the prevalence of security issues in the Nuclear Sector in the post-9/11 environment, communication protocols may need to be established between nuclear facility owners and operators, and other Federal agencies besides the NRC. Establishing these new protocols without compromising the existing lines of communication is essential to prevent confusion or dissemination of misinformation.

Because of its extensive experience in regulating the civilian Nuclear Sector and its exclusive focus, the NRC understands the sector well, and has established effective working relationships with its licensees and other stakeholders in the sector. However, there are the following challenges:

- Achieving regulatory stability in a dynamic threat environment
- Enhancing coordination and partnerships with Federal and State agencies without creating unnecessary overlap and duplication of effort

1.6 Initiatives

In order to enhance coordination and partnerships among Federal, State, and local agencies and the private sector without creating unnecessary overlap and duplication of effort, there are the following initiatives:

- DHS/CNPPD is further developing communication links and workable relationships with sector stakeholders.
- DHS/DNDO is refining and implementing the global detection architecture (building an integrated and technically proficient radiation detection system that will provide users a better capability to detect nuclear/radiological materials and weapons). DNDO will be establishing multiple pilot programs over the next several years and incorporate previous pilot program activities into the lesson learned process as well as support future efforts to appropriately test and evaluate detection technology to better understand both the technical and operational characterizations of the equipment. Finally, DNDO is establishing the Joint Center for Global Connectivity (JCGC). It will build all the necessary linkages within the Federal, State and local communities, fuse detection and other forms of data to provide a more global and comprehensive understanding of nuclear threats.

DRAFT

- In an effort to allow the exchange of classified information with licensee and industry managers, DHS and the NRC have begun sponsoring clearances for individuals who have demonstrated a need for access. For instance, DHS is sponsoring a pilot, which involves two companies receiving security clearances, safes, and courier passes to enable them to handle classified material. The DHS Office of Security and the NRC Division of Nuclear Security are in the process of negotiating a Memorandum of Agreement (MOA) between the DHS Chief Security Officer and the Director of the NRC Division of Nuclear Security. When completed, the anticipation is that this MOA would define security roles and responsibilities between the respective offices relating to classified information sharing with a specific location at each of two entities, the *Constellation Energy Group*, Baltimore, MD, and *The Nuclear Energy Institute*, Washington, D.C. Currently, the draft MOA is undergoing an informal review at the NRC.

- The NRC is in the process of negotiating classified information-exchange administrative agreements with other countries to interact on security matters of mutual interest. The NRC is working with DOS to establish contacts with new entities, develop the basis for exchanging information, and negotiate agreements under which classified information can be discussed. The NRC works under the umbrella of government-to-government security agreements for classified information exchanges.

- NEI, the NRC, and commercial nuclear power plants have established a system for the encryption of Safeguards Information to expedite sharing information of sensitive unclassified information and rapidly communicating threat information.

- The NRC has initiated actions to enhance communications. As part of the NRC chairman's initiative on communications, the NRC established a task force on public communications. The main goal of the task force is to enhance communication with external NRC stakeholders. The NRC published NUREG/BR-308, *Effective Risk Communication*, to provide guidelines for NRC staff and management to effectively communicate risk. In addition, the NRC established a communications council, which is chartered with improving internal communications.

- DHS and NRC have developed procedures whereby NRC incident response personnel staff and managers will help staff the DHS/HSOC during incidents of national significance that involve Nuclear Sector assets. In addition, DHS/HSOC works directly with the NRC Operations Center for emergency and non-emergency communication with the Nuclear Sector.

- A terrorist simulation exercise is being sponsored by the NSCC to develop a playbook to help insure government and industry coordination regarding public information released during a terrorist event.

- The NSCC is working to ensure that their essential personnel and critical nodes qualify for subscriptions to a suite of priority telecommunications services being offered by DHS/National Communications System (NCS). The suite of priority services is as follows:

  - Government Emergency Telecommunications Service (GETS) is a PIN card that gives a user priority through the public telecommunications network during times of

DRAFT

congestion. GETS is used in an emergency or crisis situation when the probability of completing a call over normal means would be significantly reduced or hampered.

- Wireless Priority Service (WPS) is a feature that gives a user priority through the cellular network on a call-by-call priority basis. The NCS executes the program on behalf of the Executive Office of the President. WPS is now available from T-mobile, Cingular, and Nextel.
- Telecommunications Service Priority (TSP) provides service vendors with an Federal Communications Commission (FCC) mandate for prioritizing restoration and provisioning on communication circuits. TSP tells the vendor what telephone lines will come up first during a National Security/Emergency Preparedness (NS/EP) event.

- ❑ The NRC has a Threat Assessment Section (TAS) that evaluates intelligence information on a daily basis, and is notified immediately of any security event involving an NRC licensee.
- ❑ The involvement of other agencies beyond the NRC in emergency exercises has been successfully broadened and deepened.
- ❑ DHS (with NRC, DOJ, and DOD support) has undertaken pilot integrated response planning activities with State and local law enforcement agencies at two reactor sites (Calvert Cliffs and Indian Point).
- ❑ An interagency steering committee was formed for developing the National Source Tracking System, discussed in sections 2, 5, and 6 of this document. Represented on the committee are the NRC (lead), DHS, DOE, the Commerce Department, DOS, and others.
- ❑ The DNDO, with interagency participation, is developing the global nuclear detection systems architecture. The architecture identifies the necessary layers and components of the global detection strategy, the functions and technical requirements of each layer and component, and a time-phased plan for strengthening the overall effectiveness of the architecture. Ultimately, it will also define in detail the information infrastructure and data standards necessary for rapid information exchange, situational awareness, and enhanced coordination between the detection and response programs.
- ❑ The DNDO will conduct pilot deployments of nuclear detection technologies with State and local users. The DNDO envisions a multi-year pilot to demonstrate a ***secure intermodal transportation corridor*** that incorporates extant radiation detector deployments along weigh stations, development and deployment of a regional data fusion center, test and evaluation of varying ConOps (including response protocols) for fixed and mobile radiation detectors, development and deployment of an appropriate communications backbone, and red-teaming exercises to challenge the success of the piloted system as a whole.
- ❑ The DNDO will conduct full characterizations of all deployed technologies. The DNDO RDT&E and acquisition process is anchored by an independent assessment of technologies as they are developed, deployed, and operated. This approach is motivated by the DNDO founding principle of fully characterizing systems (i.e. thoroughly understanding all aspects of systems performance and potential vulnerabilities) prior to

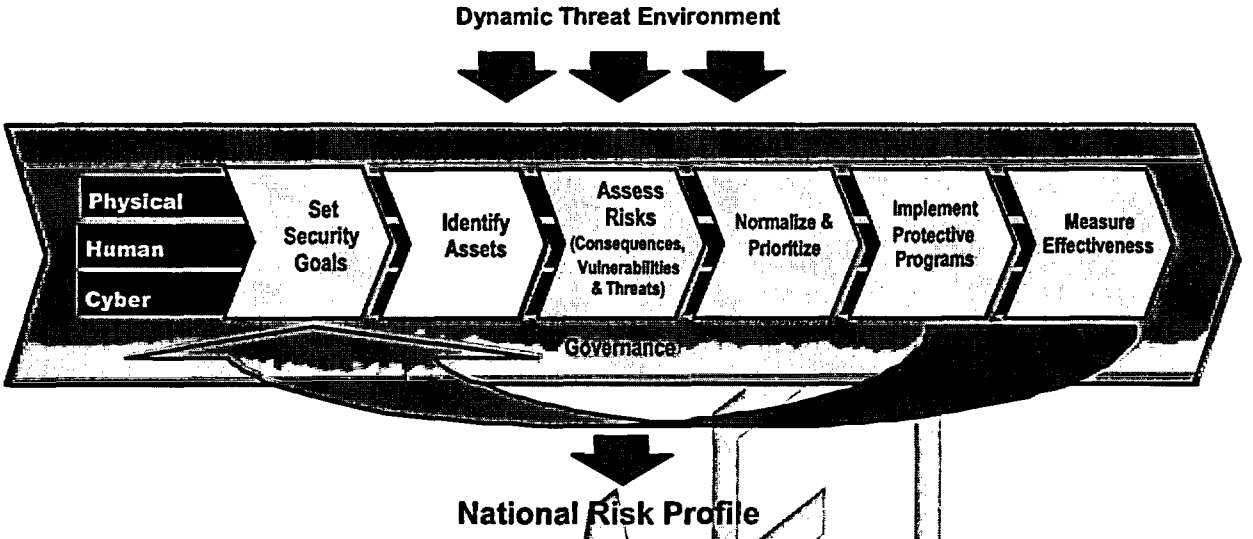
DRAFT

deploying technologies, and ensuring an accurate awareness of systems effectiveness post-deployment.

- The DNDO, under the Security & Prosperity Partnership (SPP) Agreement is working with our Canadian and Mexican counterparts to ensure the installation of radiation detection technology at major commercial and passenger ports of entry. The SPP Initiative is a multi-agency effort to support 10 goals agreed upon between the three countries. The DNDO is working with the NRC, DOS, DOE and other DHS agencies to coordinate several goals under SPP. These goals include the one noted above as well as the development of trilateral nuclear source tracking systems and the establishment of new rules and regulations within the US, Canada and Mexico that will be in line with the new IAEA Code of Conduct for import and export requirement.

DRAFT

2 Identify Assets, Systems, Networks, and Functions



There are many critical assets, systems, networks, and functions in the Nuclear Reactors, Materials, and Waste Sector. Commercial nuclear power reactors account for approximately 20 percent of the Nation's electricity-generation capacity. Any potential impact on the public or the environment will be determined by the specific nature and degree of success of the attack. On a hypothetical basis, one could assume multiple adverse impacts from a terrorist attack; for example, if a nuclear power plant was the target of a successful terrorist attack, the resulting damage could possibly result in such consequences as the release of radioactive material into the environment, contamination of local agricultural and livestock products, economic and electrical grid impacts, and potential loss of life to individuals defending the plant against the terrorists. A successful attack that shut down or compromised certain fuel cycle facilities could result in fatalities from a chemical release, theft of weapons-grade nuclear material, and/or a disruption of supplies into the defense industrial base. Additionally, the theft of certain radioactive materials in quantities of concern used in the medical and industrial fields could lead to the production and terrorist use of radiological dispersal devices (RDDs) and radiological exposure devices[18] (REDs). While the radiological impact of such devices would generally be less dangerous than the impact of the explosion itself, inherent public fear of radiation could cause widespread panic and concern in the wake of such an attack. Similarly, the psychological impact of a successful terrorist attack against a nuclear power plant or major fuel cycle facility could be significant. Other assets, systems, networks, and functions in the Nuclear Sector that must be protected include shipments of certain nuclear materials, spent nuclear fuel, and certain radioactive waste. These shipments travel between manufacturers, licensed users, and disposal facilities along the Nation's roadways, waterways, railways, and air routes.

[18] Radiological Exposure Device (RED) – A device whose purpose is to expose people to radiation, rather than to disperse radioactive material into the air, as would an RDD. An RED could be constructed from unshielded or partially shielded radioactive materials in any form placed in any type of container.

2.1 Defining Information Parameters

The regulatory process identifies sector assets. The formal licensing reviews ensure that nuclear facilities and entities using, acquiring, transporting, or disposing of radioactive materials in quantities of concern are identified and assessed. Indeed, a license is required prior to any entity receiving radioactive materials in quantities of concern or operating a civilian nuclear facility.

The Nuclear Sector is divided into the following categories:

Table 4: Nuclear Sector[19]

NUCLEAR POWER PLANTS
- A. Light Water Reactor Power Plants
- B. Other Reactor Power Plants

RESEARCH AND TEST REACTORS
- A. Government Research and Test Reactors
- B. University Research and Test Reactors
- C. Private Research and Test Reactors

NUCLEAR FUEL CYCLE FACILITIES
- A. Uranium Mining or In Situ Uranium Leaching
- B. Uranium Ore Milling or Leachate Processing
- C. Uranium Conversion Facilities
- D. Uranium Enrichment Facilities
- E. Fuel Fabrication Facilities
  1. Category I (Special Nuclear Materials) Facilities
  2. Category II (Special Nuclear Materials – Moderate Strategic Significance) Facilities
  3. Category III (Special Nuclear Materials – Low Strategic Significance) Facilities

RADIOACTIVE WASTE MANAGEMENT
- A. Low-Level Radioactive Waste Processing and Storage Facilities
- B. Sites Managing Accumulations of Naturally Occurring Radioactive Materials (NORM)
- C. Spent Nuclear Fuel Processing and Storage Facilities
  1. Spent Nuclear Fuel Wet Storage Facilities
  2. Spent Nuclear Fuel Dry Storage Facilities
- D. Transuranic Waste Processing and Storage Facilities
- E. High-Level Radioactive Waste Storage and Disposal[20] Facilities

NUCLEAR MATERIALS TRANSPORT
- A. Low Hazard Radioactive Materials Transport
- B. High Hazard Radioactive Materials Transport

DEACTIVATED NUCLEAR FACILITIES
- A. Deactivated Reactors
- B. Other Deactivated Nuclear Facilities

RADIOACTIVE MATERIAL USERS
- A. Medical Facilities with Radioactive Materials
- B. Research Facilities with Radioactive Materials

DRAFT

[19] The order in which the subsectors in this table are listed does not reflect the amount of risk, threat, vulnerability, or consequence associated with the types of assets in regard to a terrorist attack.

[20] For item E for "radioactive waste management", the NADB currently states "High-Level Radioactive Waste Storage Facilities." *However, a modification plans to be made so item IV.E reads "High-Level Radioactive Waste Storage and Disposal Facilities."*

C. Irradiation Facilities
D. Industrial Facilities with Nuclear Materials
E. Radiopharmaceutical and Medical Isotope Production Facilities
F. Radiographers, Well Loggers, and Portable Density Gauge Users[21]

RADIOACTIVE SOURCE PRODUCTION AND DISTRIBUTION FACILITIES
A. Radioactive Source Importers
B. Radioactive Source Manufacturers

REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
A. Federal Nuclear Agencies
B. Regional, State, and Local Nuclear Agencies
C. Nuclear Industry Organizations

OTHER NUCLEAR FACILITIES

In order to facilitate the compilation and management of the Nation's infrastructure data, DHS created the National Asset Database (NADB). The NADB is the Federal government's repository for information on the evolving, comprehensive inventory of assets that make up the Nation's infrastructure. The NADB is not a prioritized list of the Nation's critical infrastructure, but the data contained therein is searchable in a variety of ways, and can be used to create prioritized lists based on selected parameters.[22] The NADB categorizes assets by sector, subsector, and segment classification, with the broad sector designations modeled after the seventeen CI/KR sector taxonomy used in HSPD-7. Currently, over 90,000 assets have been identified from a variety of sources and, once the data on a given asset is verified, the asset is added to the NADB.

As a first step in identifying sector assets, DHS must define the specific types of information that it seeks to collect about each asset. The selected data categories will become data fields contained within the NADB and must be broad enough to support the entire range of CIP activities for which the NADB serves as an asset identification source. In determining what data will be sought for assets contained in the NADB, DHS will take a comprehensive, integrated view of the asset including all of its characteristics and the cross-sector CI/KR dependencies necessary for it to function. This is necessary because the functionality of many assets are dependent on multiple elements and systems (e.g., people, physical, information technology, telecommunications), and it is these elements, as well as asset interdependencies, that will provide the basis for assessing potential consequences, vulnerabilities, and risks, and developing protective strategies.

Within the NADB, certain information is sought for all assets regardless of sector, subsector, or segment, while additional information may be sought only for particular asset types. Some of the data fields that apply to all assets, regardless of asset type, include:

- Asset name, address, and local contact information
- Geographic location (e.g., latitude/longitude, global positioning system (GPS) coordinates; distance to nearest major metropolitan area)

[21] Items E and F under "radioactive material users" have not yet been added to the NADB, but will likely be added in the near future.

[22] The NADB has been used for this purpose on numerous occasions to date, and has served as the foundation for developing programmatic focus for a variety of various DHS initiatives by identifying critical assets to be targeted by those initiatives. Those initiatives include the Buffer Zone Protection Program (~1800 assets), Site Assistance Visits (~220 assets), Project Sentinel (~440 assets), the Interagency Security Program (~800 assets), and the Urban Area Security Initiative (~8000 assets).

- ❑ Classification/taxonomy information (e.g., sector, segment, attribute)
- ❑ Owner/operator name, address, and type (e.g., public, private)
- ❑ Chief Executive Officer name and address (if applicable)
- ❑ Chief Security Officer name and address (if applicable)
- ❑ Parent company (if applicable)
- ❑ Physical structure information (e.g., square footage, seating capacity, number of floors, building height)
- ❑ Business identification codes and ratings (e.g., North American Industry Classification System (NAICS), EPA Facility ID, Dun & Bradstreet rating)
- ❑ Congressional information (e.g., Congressional district, Representative, Senator)
- ❑ Cyber elements (e.g., distributed control systems (DCS), process control systems (PCS), supervisory control and data acquisitions (SCADA) systems; access control databases)
- ❑ DHS program information (e.g., Protective Security Advisor (PSA) district; BZPP status)

Licensing is one way that the NRC gathers information about assets in the Nuclear Sector. The regulatory categories are covered in Section 1.1. There is a broad range of types of licenses and the criticality of the assets is quite variable. The factors to determine if an asset is considered an asset of consequence for DHS include: potential casualties, economic impact, and other societal consequences.

The NRC licenses the design, construction, operation, and decommissioning of commercial nuclear plants and licenses other nuclear facilities, such as nuclear fuel facilities, uranium enrichment facilities, and nonpower reactors. When the NRC receives a license application for a civilian nuclear reactor, one of the items that the NRC reviews is safety related information and control (I&C) systems to ensure that they meet the NRC's regulations. The NRC also licenses the siting, design, construction, operation, and closure of low-level radioactive waste disposal sites under NRC jurisdiction and the construction, operation, and closure of a geologic repository for high-level radioactive waste. Beyond that, the NRC licenses the possession, use, processing handling, and exporting of nuclear materials and the operators of civilian nuclear reactors.

In addition to data collected through the NADB and the NRC, asset information will be collected by the SSA who will be responsible for identifying and obtaining data for the assets, systems, and networks that involve significant dependencies, interdependencies, or critical functionality. The SSA will also work with specific countries to identify international interdependencies and vulnerabilities as well as to maintain and protect information on foreign critical infrastructure and resources.

2.2 Collecting Infrastructure Information

In order to use nuclear materials above a low threshold or operate a facility that uses nuclear materials, the NRC or an Agreement State must license an entity or individual. The NRC or Agreement State reviews the information submitted by the applicant using standard review plans to ensure that the applicant's assumptions are technically correct, and that the environment will not be adversely affected by a nuclear operation or facility.

DRAFT

The NRC licenses the design, construction, operation, and decommissioning of nuclear plants and licenses other nuclear facilities, such as nuclear fuel facilities, uranium enrichment facilities, and nonpower reactors. The NRC also licenses the siting, design, construction, operation, and closure of low-level radioactive waste disposal sites under NRC jurisdiction and the construction, operation, and closure of a geologic repository for high-level radioactive waste. Beyond that, the NRC licenses the possession, use, processing handling, and exporting of nuclear materials and the operators of civilian nuclear reactors.

Once a facility's license is approved and operations commence, the NRC or Agreement State agency continues to regularly collect data for use in effective regulation. The NRC has a comprehensive program of inspections for commercial nuclear power plants, fuel cycle facilities and RTRs. Generally, inspectors verify that the operation, operator qualifications, design, maintenance, safety, security, fuel handling, material control and accounting (MC&A), and environmental and radiation protection programs are adequate and comply with NRC safety requirements.

In addition, the NRC conducts roughly 2,000 inspections of nuclear material licensees per year. These inspections cover such areas as the training of personnel who use materials, radiation protection programs, radiation patient dose records, and security of nuclear materials. The Agreement States conduct comparable inspections of the thousands of material licensees that they regulate.

The reporting requirements of Title 10 of the Code of Federal Regulations require that all licensees and Agreement States report certain events and conditions to the NRC. These event reports have specific time criteria for notification to the NRC Operations Center. This information is used by the NRC staff to identify threats or respond to emergencies, monitor ongoing events, study potentially generic safety and security problems, monitor performance, identify precursors of more significant events, and recognize inadequacy or unreliability of specific equipment or procedures.

Also, the NSCC-Radioisotope Subcouncil (NSCC-R) has prepared an inventory of applications corresponding to typical radionuclides and activity for the purpose of prioritizing these on the basis of risk. The NRC has vetted this inventory.

2.2.1 DHS Data Collection for NADB

Historically, DHS has used a variety of means for gathering data on the Nation's infrastructure. In 2004, DHS issued a data call to State Homeland Security Offices asking the States to identify CI/KR located within their borders. Similarly, as part of Project Matrix, DHS requested information from other Federal agencies in an effort to collect data on government facilities located throughout the Nation. In addition to these broad data calls, DHS has coordinated with individual governmental entities to gain access to CI information collected in response to statutory and other requirements. For instance, EPA has shared with DHS information it collected as part of its Risk Management Plan (RMP) program, and the U.S. Coast Guard has shared with DHS information submitted in compliance with the Maritime Transportation Security Act (MTSA).

In addition to working with States and other Federal entities, DHS has collected some asset data by working directly with asset owner/operators. During the implementation of various initiatives, such as Comprehensive Reviews (CRs) and Buffer Zone Protection Plans (both of

DRAFT

which are discussed further in Chapter 6), DHS learns valuable information concerning risk-significant critical infrastructure directly from asset owner/operators or local law enforcement and other emergency response personnel. Similar information is garnered when DHS works with asset owner/operators when specific threat intelligence causes DHS to tactically respond to assist in securing select facilities. The knowledge acquired about risk-significant CI/KR during both strategic and tactical operations performed by DHS is catalogued and maintained in the NADB.

2.2.2 Future DHS Data Collection Efforts within the Nuclear Sector

DHS and the NRC are working to develop a partnership in the sharing of asset information in the Nuclear Sector. As the NRC has information on numerous assets within the sector, DHS is defining the criteria on which assets would be most useful to have within the NADB. The NRC has provided necessary asset information to DHS, and will provide updates to it on an annual basis or more frequently as needed. The NRC and SSA will also work together to facilitate the formatting of NRC and any other industry databases into the NADB format including using a standardized format, data scheme, and categorization system or taxonomy defined by DHS. The SSA will create a schedule for importing necessary data and will biannually conduct a review the information in the database to verify its accuracy.

Another future effort will include DHS/SSA gathering and protecting information on the foreign infrastructure on which the Nuclear Sector in the United States depends.

2.2.3 Use of Infrastructure Information

As the Risk Management Framework diagram shows, collecting information on assets, systems, networks, and functions is a prerequisite to being able to determine the risk associated with them. Risk assessment then leads to prioritization among the assets, systems, networks, and functions, which helps determine where protective actions should be taken.

2.3 Verifying Infrastructure Information

Once an applicant for a license has submitted an application for nuclear facility operation, or possession and use of special nuclear material, the NRC staff reviews the application to determine that it meets all applicable regulations. For power reactors and Category I fuel cycle facilities, the application must include the licensee's safeguards contingency plan, containing plans for dealing with threats, thefts, and radiological sabotage related to the special nuclear material and nuclear facilities being licensed. The application must also include a physical security plan, and a guard qualification and training plan. When the NRC completes its review and evaluation, it prepares a safety evaluation report (SER), which summarizes the anticipated effect of the proposed facility on public health and safety. The NRC has reviewed and approved the physical security plans, guard qualifications and training plans, and contingency plans submitted in compliance with NRC's April 29, 2003 orders for all power reactors.

The ACRS, an independent group that provides advice on reactor safety, not security, to the NRC's five-member Commission, independently reviews each application to construct or operate a nuclear power plant. The ACRS review begins early in the licensing process, and a series of meetings with the applicant and the NRC staff are held at appropriate times in the review process. When the Committee has completed its review, its report is submitted to the Commission via a letter to the chairman of the NRC.

DRAFT

Individuals or entities directly affected by any licensing or enforcement action involving a facility that produces or uses nuclear materials generally may request a hearing before independent judges on the ASLBP. The panel conducts licensing and other hearings as directed by the Commission, primarily through individual atomic safety and licensing boards or single presiding officers appointed by either the Commission or the chief administrative judge. The panel, which has no fixed number of positions, is composed of administrative judges (full-time and part-time), who are lawyers, engineers, and scientists. Administrative judges serve as single presiding officers or on three-member boards, which generally are chaired by a lawyer, for a broad range of proceedings.

An entity applying for a specific license to use nuclear materials will also submit an application to the NRC. For materials licensees, the NRC's goal is to obtain detailed data on the materials possessed by each licensee, based on radioactivity thresholds. These thresholds help to determine the point at which a licensee holds an amount of a given isotope sufficient to cause harm due to accidental exposure or malicious use. This process will be discussed in more detail in later sections of this document.

2.3.1 Review of Submitted Material

The NRC's program offices employ technical staff who are well-versed in all aspects of facility operations, licensing, security, and nuclear material safety and safeguards. When NRC licensees submit material for review, the technical staff assesses the submittal, ensures that it addresses the correct safety, security, and regulatory issues, and either approves or rejects the licensee's request. This process often involves requests for additional information from the NRC back to the licensee, meetings, and conference calls.

2.3.2 Inspection Process

Inspections are an important element of the NRC's oversight of its licensees. The NRC conducts inspections to ensure that licensees satisfy regulatory requirements, and operate in a manner that protects the public and the environment from any undue nuclear risk. During the inspections, information about the assets previously collected is verified, and this is fed back to the NRC databases that store that type of information.

2.3.3 Data on Radioactive Materials

The U.S. Government has a national data base for tracking uranium, thorium and plutonium: the Nuclear Materials Management and Safeguards System (NMMSS). NRC and Agreement State licensees report to NMMSS when they receive, ship, or perform an inventory of uranium, thorium, and plutonium. In 2004, all NRC licensees with material registered in NMMSS were requested to inventory their material and ensure the accuracy of the data recorded in NMMSS. In 2005, selected NRC and Agreement State licensees' submittals to NMMSS were verified during onsite inspections.

Additionally, the NRC and DOE are spearheading a larger initiative to inventory and maintain a database for risk-significant radioactive sources held by NRC and Agreement State licensees, and DOE facilities in excess of certain thresholds. This initiative involves sending a survey form to materials licensees authorized to use the types and amounts of radiological materials above threshold quantities. The purpose of this initiative is to identify the possession and location of materials of greatest concern for use in an RDD. The results from the study are being used to

DRAFT

determine whether additional measures should be taken to protect these materials. The information is maintained in an interim database, which is expected to be replaced by the National Source Tracking System upon adoption of a final rule and deployment of the required internet-linked database software system.

2.4 Updating Infrastructure Information

The NRC issues licenses to private sector entities and governmental agencies in the nuclear subsectors defined in Section 1.1. The licensing certification process ensures that any new assets coming into the sector are licensed and properly tracked.

The NRC Operations Center staff is on duty 24 hours per day, and concurrent with their other responsibilities, is able to receive information on changes in the status of assets.

Once it is populated, NRC and DOE will use the National Source Tracking System to periodically update the quantities and types of risk-significant nuclear material held by their licensees.

In this sector, the NRC provides asset information to the SSA and DHS's NADB on a regular basis, upon request, and when time-sensitive information becomes available. This information is protected based on guidelines explained in Section 2.5. The NRC's Office of Nuclear Security and Incident Response is the focal point for interactions with the SSA. On a biannual basis, the SSA conducts a maintenance review of the asset information in the NADB, verifying the accuracy of the NADB's information.

2.5 Protecting Infrastructure Information

Due to the sensitive nature of some information that the private sector provides to the government, there are various ways that information can be exempt from public disclosure. Having this protection in place makes the private sector more willing to share important information with the government, and this allows the government to make more educated decisions in determining risk to specific assets, systems, networks, and functions within the sector and the sector as a whole. Some of the ways that information can be protected includes the Protected Critical Infrastructure Information (PCII) Program, categorizing information as Safeguards Information (SGI), and classifying information.

2.5.1 PCII Program

The Protected Critical Infrastructure Information (PCII) Program creates a framework that enables the private sector to voluntarily submit sensitive and proprietary information about the nation's critical infrastructure to the government. Congress passed the Critical Infrastructure Information Act of 2002 (CII Act) to enable private industry to share valuable security-related information without compromising it. The CII Act provides protection for qualified CII from disclosure under the Freedom of Information Act (FOIA) and State and local open records laws, and from use in Federal or State civil litigation.

The PCII Program Office, created by DHS to implement and manage the PCII Program, evaluates voluntarily submitted critical infrastructure information to determine whether it qualifies for protection under the CII Act. PCII may be used for many homeland security purposes,

DRAFT

focusing primarily on analyzing and securing critical infrastructure and protected systems, risk and vulnerabilities assessments, and assisting with recovery efforts.

There are several benefits of using the PCII Program to share CII.

- Proprietary or business-sensitive infrastructure information can now be shared with government entities with the legal presumption of protection from public disclosure
- Allows industry to share CII with several government entities through a single submission reducing the need for multiple data requests
- Information sharing will result in better identification of risks and vulnerabilities, which will help industry partner with government in protecting key assets
- Information is protected through numerous mechanisms including government user training and handling requirements to access the data

Submissions may be made via fax, mail, courier or through a secure Web portal accessed from the PCII Program Web site, http://www.dhs.gov/pcii. The PCII Web site also has the latest Program information and instructions on how to participate.

2.5.2 Classified Information

Information classified in regard to the Nuclear Sector is primarily of two types:

- ❑ **National Security Information (NSI):** Information classified by an Executive Order, whose compromise would cause some degree of damage to the national security.
- ❑ **Restricted Data (RD):** Information classified by the Atomic Energy Act, whose compromise would assist in the design, manufacture, or utilization of nuclear weapons.

Several levels of classified information include Top Secret, Secret, and Confidential.

Access to classified information requires a personnel security clearance equal to or higher than the level of information and a need-to-know.

2.5.3 Safeguards Information (SGI)

Safeguards information is a special category of sensitive unclassified information authorized by Section 47 of the Atomic Energy Act to be protected. Safeguards information concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.

While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified Confidential information than other sensitive unclassified information.

The categories of individuals who are permitted access to SGI are listed in 10 CFR 73.21.

DRAFT

2.6 Challenges

2.6.1 Materials Tracking/Inventory

With almost 2,000 materials licensees possessing risk-significant radioactive material, about a third of whom are NRC-regulated, and the remainder of whom are Agreement State-regulated, the sector is challenged to acquire and update an accurate database of the risk-significant radioactive materials possessed by its licensees. In many cases, organizations hold active materials licenses, but no longer have radioactive material on hand. In order to effectively protect the public, the NRC must keep this information as accurate and up to date as possible without impeding the safe use of the sources.

2.6.2 Telecommunications Dependencies

The NRC has, for many years, routinely tested notification and response communications systems with reactor licensees and some fuel cycle licensees. NRC and Agreement State communication with materials and transportation licensees are less established and tested. Commercial telephone lines represent the primary form of communications, although wireless and Internet media are used on a more frequent basis. Each communication medium depends on other critical infrastructures, such as the availability of electricity from the grid, and alternate or emergency power supplies. All reactor sites and some fuel cycle facilities have alternate and emergency power capability.

Commercial landlines and cell phones are not secure methods of communication. The changing threat environment in the sector has brought about the need for secure means of communicating vital data associated with potential threats to sector assets, systems, networks, and functions.

2.7 Initiatives

In order to accurately track the use of risk-significant radioactive materials, and to ensure the validity of new license applicants, there are the following initiatives:

- The NRC has completed the development of an interim database of risk-significant radioactive material held by NRC and Agreement State licensees. Annual updates of the database will continue to be made until the National Source Tracking System is fully operational.
- The NRC is beginning the process of revising its MC&A regulations.
- The NRC and DOE are working together to review current reporting requirements to the NMMSS database to ensure more commonality between the requirements of the two regulatory agencies while maintaining the validity of licensee reports concerning special nuclear material.
- The Energy Policy Act of 2005 expanded the requirements for fingerprinting and background checks to include applicants for licensing or certification. The NRC is considering a pre-application verification process that will validate the legitimate need of an applicant to obtain radioactive materials in quantities of concern. This process may involve an inspection prior to receiving sources of concern, to ensure that they will be used in an appropriate manner.

DRAFT

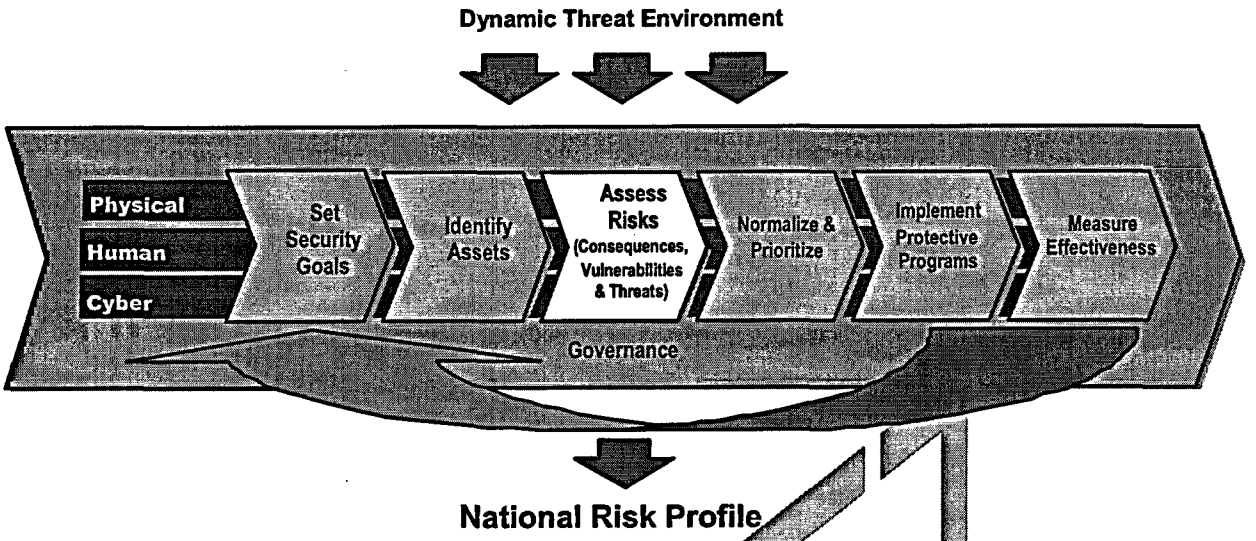
- ❑ The DHS/SSA is working with the NRC, DOE, EPA, and Health and Human Services as necessary to implement source-strength threshold criteria for inclusion as assets, source tracking, and protective measures. The guidance documents for categorizing sources are IAEA TECDOC-1344, Categorization of Radioactive Sources, and the IAEA Code of Conduct for the Safety and Security of Radioactive Sources.
- ❑ The NRC is revising the CFR rules to track radioactive materials in quantities of concern
- ❑ The NRC revised 10 CFR 110, which governs the import and export of radioactive materials in quantities of concern.
- ❑ The NRC has issued a proposed rulemaking to set out more detailed requirements in many areas of the Fitness-for-Duty (FFD) program, including:
    - Requiring validity tests for urine samples to detect tampering
    - Tougher sanctions for violations, including permanent denial of unescorted access for refusing, or attempting to subvert a test
    - Adding Substance Abuse Experts to licensee staff
    - Codifying individual work hour limits for certain workers
    - Establishing minimum individual breaks between shifts, and on a bi-weekly basis
    - Establishing maximum weekly work schedules for certain groups while the plant is operating

In order to meet its telecommunications challenges with the NRC and other Federal/State/local stakeholders, there are the following initiatives:

- ❑ Requiring some licensees to have wireless communications systems to serve as a backup method for contacting the NRC when commercial lines are not available
- ❑ Maintaining reliable phone lines (emergency notification system) with all reactor plant licensees. Many reactor licensees use long-distance telephone lines managed by the Federal Telecommunications Service (FTS 2001) contract. The NRC facilitates the repair of vital licensee telephone lines under this contract by submitting and tracking trouble calls on any lines that experience problems.
- ❑ Installing secure telephones and faxes at key locations in NRC facilities and field locations to facilitate secure communication with power reactor and Category I fuel cycle facility licensees, other agencies, and among NRC offices

DRAFT

3 Assess Risks



The Department of Homeland Security will continue to coordinate security risk analyses with other Federal agencies that relate to the activities in this sector. Consistent with the Homeland Security Act, DHS utilizes three major components in its evaluation of risk: threat, vulnerability, and consequence. Threat can be described as the probability of attack on the facility under consideration. Vulnerability is the probability that the attack will be successful. Consequence is some measure (lives, dollars, etc.) of the damage that would result from a successful attack. Threat and vulnerability are not absolute probabilities; it is important only that they be normalized within the set of threats and vulnerabilities used for comparison in the analysis. Risk is the function of these three components, and has the same units as the measure of consequence. In order to make more educated risk assessments, DHS often relies on the private sector to perform vulnerability, consequence, and threat (or attractiveness) analyses on their facilities.

The NRC also needs to perform risk assessments in order to determine what regulatory measures to put in place. Following the September 11, 2001 attacks, the NRC Commissioners directed an in-depth review of safeguards and security for the Nuclear Reactors, Materials, and Waste Sector. The NRC developed a plan for the in-depth review of safeguards and security programs for NRC-licensed facilities and activities, which described the three-step process that the NRC is following: (1) threat definition; (2) security assessments (SAs); and (3) regulatory improvements.

3.1 Use of Risk Assessment in the Sector

The Risk Analysis and Management of Critical Assets Protection (RAMCAP), described below, is one methodology that the Nuclear Sector is utilizing. However, other methodologies are also options, and Appendix 3A of the NIPP addresses the NIPP baseline criteria for assessment methodologies. While that appendix describes the criteria in detail, two important characteristics of an acceptable methodology are credibility and comparability with other methodologies. In order for a methodology to be credible, it needs to address the consequence,

DRAFT

vulnerability and threat aspects of risk. It needs to be complete, in that it provides reasonably complete results via a quantitative, systematic, and rigorous process. The methodology must also be defensible, in that it uses recognized methods of the professional disciplines relevant to the analysis and adequately addresses the relevant concerns of government, the CI/KR work force, and the public. For a methodology to be comparable with other methodologies, it needs to be documented, transparent, reproducible and accurate.

When performing risk assessments in the Nuclear Sector, most assessments will focus on a specific asset or category of assets within the sector, such as a commercial nuclear power plant or a site where radiological materials are used for medical purposes. However, in a few instances, performing a system-based risk assessment will provide additional value. For instance, the transportation of nuclear and radiological materials involves a collection of assets and resources working together to move the material, and can be analyzed in this fashion. Also, the collection of equipment that detects nuclear and radiological material used to prevent unauthorized material from entering this country, which is deployed throughout the country, is best viewed as a system, and can be analyzed in this way.

3.1.1 Risk Analysis and Management of Critical Assets Protection (RAMCAP)

RAMCAP is an effort to develop common criteria for conducting strategic risk analyses that can be applied across all 17 CI/KR sectors. Common criteria include: use of common terminology and reporting for defining Asset and Threat Characterization, Consequence and Vulnerability Analysis, Threat and Risk Assessment, and Risk Management. RAMCAP provides a common, non-sector specific, reporting framework, enabling informed resource allocation and consequence mitigation decisions. The application of RAMCAP across the 17 CI/KR sectors will enable a more informed positioning of local and regional response capabilities to threats extending beyond the NPP site.

The purpose of RAMCAP is two-fold. First, develop general vulnerability and strategic risk assessment guidelines that can be used as the basis for assessments on assets in all CI/KR sectors. Second, develop comparative risk analysis guidelines that can then be used to normalize and compare assets from different sectors and allow asset prioritization for protection of our nation's CI/KR. The NPP supports the utilization of RAMCAP as an appropriate risk assessment methodology.

In order to be successful, RAMCAP must be developed by industry for industry; therefore DHS has reached out to the private sector to develop RAMCAP. The American Society of Mechanical Engineers (ASME) is coordinating the creation of a RAMCAP document that provides guidance on approaches and methodologies for: analyzing strategic risks associated with adversary attacks; identifying and developing countermeasures and consequence-mitigation strategies to reduce risks; and evaluating countermeasures and consequence-mitigation strategies using cost-benefit analyses and other methods to inform resource allocation decisions.

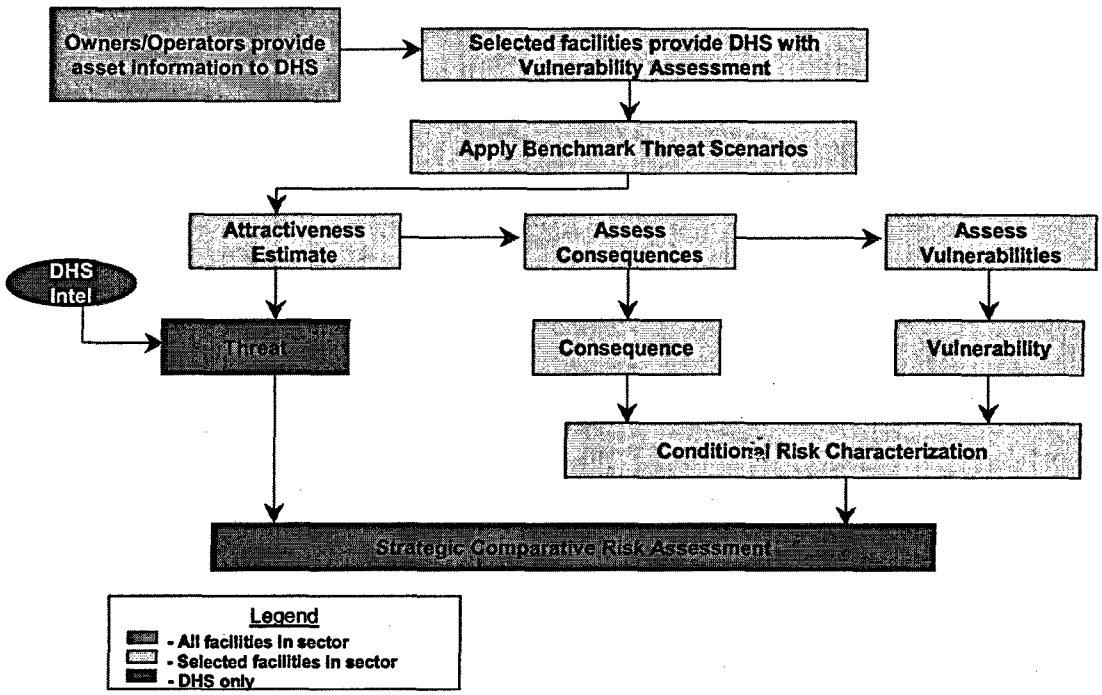
The guidance in the document is intended to be broadly applicable to all sectors. Modules will be developed based on a RAMCAP Master Template that will provide sector, sub-sector, or segment specific guidance. RAMCAP is being currently used in the Nuclear Sector and is being piloted in the Chemical Sector. Other sector module sets will follow.

DRAFT

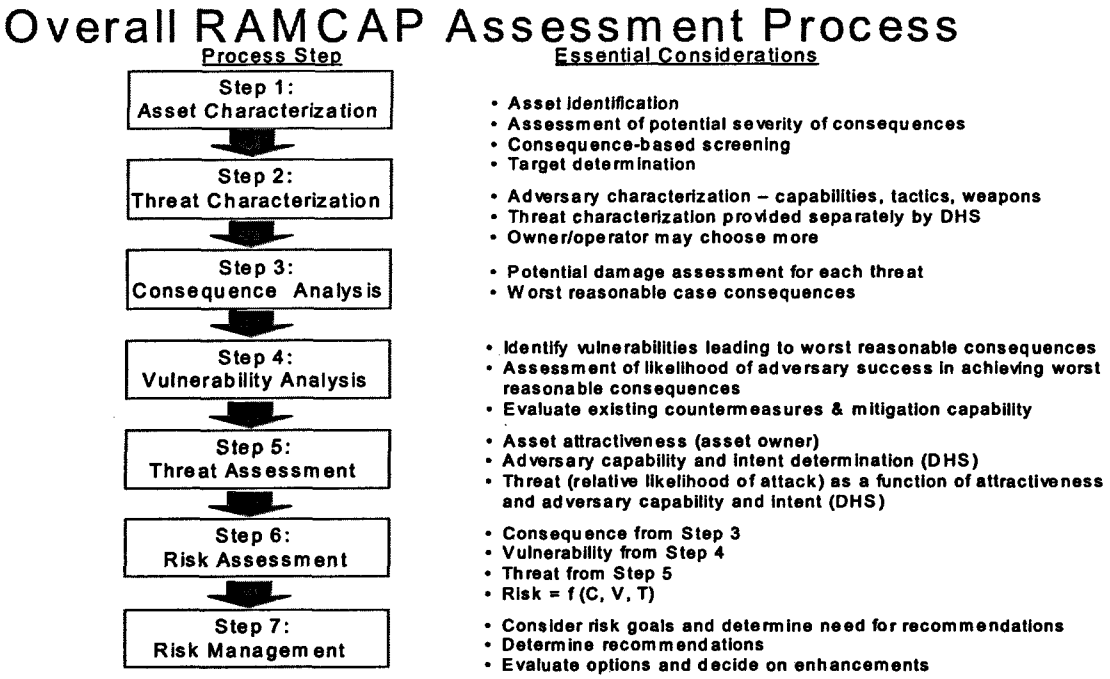
As part of the Nuclear Comprehensive Review (CR) process, industry presents any available RAMCAP results for a given site during the CR preparation week. This information significantly assists the CR team in identifying any particular items of interest for the onsite week of the CR.

RAMCAP results allow DHS and other Federal agencies to prioritize assets from different sectors based on comparative risk analyses. This will in turn allow DHS and other agencies to implement protective measures and employ our nation's resources in a manner that maximizes the allocation of limited resources for the security of the nation.

RAMCAP Process



Implementing new protective measures can have an impact on the vulnerabilities, consequences and attractiveness of a terrorist attack on a facility. If additional protective measures of a significant nature are implemented, then reassessing attractiveness, consequences and vulnerabilities should be considered.



3.1.1.1 Step 1: Asset Characterization

Asset characterization and screening analyzes the technical details and operational processes of a facility to identify critical assets and hazards and forecasts potential consequences from a terrorist act. In the Nuclear Sector, the hazards being considered include a radiological release, the impact on the electric grid, and transportation issues. The assets evaluated include those on the facility as well as its surrounding and supporting infrastructure. The analysis includes identification of existing layers of protection. This analysis differentiates between those assets that produce a significant impact as a result of a terrorist act and should be reported to DHS and those assets that remain primarily the concern of the asset owner/operator.

3.1.1.2 Step 2: Threat Characterization

Threat characterization seeks to identify specific and general modes of attack that may be used by terrorists against a given target. Asset owners/operators, who implement RAMCAP strictly for their own decision-making, may define scenarios as they choose. However, for risk knowledge to be useful to DHS, comparisons must be made based upon a common set of defined threat scenarios. This set of scenarios is provided by DHS. DHS bases its characterizations on the collective activities of law enforcement and intelligence organizations that are charged with developing an understanding of the means, methods and motivations of terrorists. These efforts are aided by the in-depth facility knowledge and perspective of the facility operator, whose own analysis may identify threats not readily recognized by DHS. These threats include various modes of attack (e.g., air, land, and water), and various sizes of attacks (small, medium, and large) with supplemental details to judge impact. Not all threats apply to every facility. Some threats will be screened out from further consideration.

3.1.1.3 Step 3: Consequence Analysis

Consequence analysis identifies the worst reasonable consequences that could be generated by a specific threat. This step looks at facility design, layout and operation in order to identify the types of consequences, particularly from a radiological release, that might result. Both causality, both on-site and off-site, and financial impacts, such as the costs of radiological clean up, resulting from different damage scenarios are calculated.

3.1.1.4 Step 4: Vulnerability Analysis

Vulnerability analysis seeks to determine the strength or weakness of a potentially targeted asset and its protective systems to a specified threat. This involves analyzing the existing capabilities and countermeasures at the asset or facility and their effectiveness in reducing those vulnerabilities.

3.1.1.5 Step 5: Threat Assessment

Asset attractiveness assessment considers the perceived value to the terrorist of attacking a given facility considering the deterrence value of security measures and the robustness of the potential target. This is assessed by the owner/operator. Threat assessment is performed by DHS and includes normalized assessments of attractiveness in light of the high level objectives of terrorists and intelligence based assessments of adversary capabilities and intent.

3.1.1.6 Step 6: Risk Assessment

Risk assessment is a systematic and comprehensive evaluation of the previously developed terrorism related data for a given facility. The owner/operator risk assessment creates a foundation for selecting strategies and tactics to defend against terrorist attacks by establishing priorities based on risk. The risk assessment utilizes the results from the consequence analysis, vulnerability analysis and threat assessment steps.

3.1.1.7 Step 7: Risk Management

Risk management is the deliberate process of understanding risk and deciding upon and implementing action, e.g., defining security countermeasures, consequence mitigation features or characteristics of the asset, to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by identifying, measuring and controlling risks to a level commensurate with an assigned or accepted value.

3.1.2 NRC Process

The NRC's three-step process for the in-depth review of safeguards and security programs for NRC-licensed facilities and activities involves: (1) threat definition; (2) security assessments (SAs); and (3) regulatory improvements.

Historically, NRC security regulations have been based largely on deterministic analyses developed without the benefit of quantitative or measurable estimates of risk. Most of these analyses have focused on failures of engineered or administrative controls. The security analyses and SAs complement the deterministic analyses by introducing a new set of initiating conditions. Most NRC regulatory requirements for nuclear reactors were developed in the early

DRAFT

stages of reactor technology development, and thus were based on limited experience, testing programs, and expert judgment, in conjunction with conservative design margins and the defense-in-depth philosophy to protect public health and safety. The deterministic approach asks two questions: (1) What can go wrong? and (2) What are the consequences? This approach assumes that adverse conditions can occur, and requires plant designs to include safety systems capable of preventing or minimizing accident consequences.

In the past decade, both the NRC and the nuclear power industry have recognized that probabilistic risk analysis (PRA) has evolved to the point that it can be used increasingly as a tool in regulatory decision-making. In 1995, the NRC adopted a PRA policy statement which directs that "the use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."

In addition to the deterministic approach questions "what can go wrong?" and "what are the consequences?" the PRA approach asks an additional question: "how likely is it that something will go wrong?" Applying this additional factor of likelihood to the threat and accident analysis process is known as risk-informing the process. By risk-informing the process, the NRC can focus its regulatory efforts on protecting the public from the events that (1) result in adverse consequences, and (2) are the most likely to occur.

3.1.3 Cyber Security in the Nuclear Sector

In September 2002, the NRC initiated a cyber assessment project with technical assistance from Pacific Northwest National Laboratory (PNNL). Participants in the project included four commercial nuclear power plants, NRC staff members, and industry. The primary objective of this project was to develop a cyber security self-assessment method that can be used by NRC licensees to assess and manage cyber risks at their plants. The focus of the cyber security self-assessment method is on *critical digital assets* (CDAs), defined as a digital device or system that plays a role in the operation or maintenance of a critical system or can impact the proper functioning of that system. A critical system is any system that, if compromised, could adversely impact the safety, security, and emergency response of a nuclear power plant. The secondary objective of the project was to document generically applicable observations made at the four pilot plants while developing this cyber security self-assessment method and to recommend potential cyber security improvement measures that NRC licensees may find useful in addressing those documented observations.

The NRC completed the project in October 2004, and documented the results in technical reports NUREG/CR 6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants," and NUREG/CR 6852 "An Examination of Cyber Security at Several U.S. Nuclear Power Plants." Using NUREG 6847 as a foundation and the insight gained during the project, the industry task force developed Nuclear Energy Institute(NEI) 04-04 "Cyber Security Program for Power Reactors," to provide nuclear power reactor licensees a means for developing and maintaining effective cyber security programs at their sites. In December 2005, the NRC accepted NEI 04-04, Revision 1, as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants.

In 2006, the NEI expects to recommend that all power reactor licensees implement a cyber security program per NEI 04-04, Revision 1, at their plants within the next two years. NEI's

expected recommendation is in line with objective #5.1, which is to implement the NRC recommended cyber security programs at all the commercial nuclear power plants. The NRC plans to continue to interact with the Task Force to encourage licensees to voluntarily implement NEI 04-04. The NRC and the nuclear industry, including international security partners, will continue to collaborate and share information on cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Additionally, the NRC is currently developing proposed rule language to ensure that power reactor licensees establish and maintain an effective cyber security program at their plants.

The SSA, DHS/CNPPD, will work with the other stakeholders in the Nuclear Sector to establish mutual assistance programs for cybersecurity emergencies.

3.1.4 Securing Risk Assessment Information

When appropriate, risk assessment information will be protected utilizing one of the various methods available to DHS or the NRC, due to the information's sensitivity. These methods, described in more detail in section 2.5, include categorizing the information as PCII, SGI, or classified.

3.2 Screening Infrastructure

Screening enables a determination to be made whether a more detailed review of a specific portion of the infrastructure should occur to determine the amount of risk associated with it. If the infrastructure is below a certain threshold of risk with a high-level analysis, then resources are better spent further analyzing other portions of the infrastructure that are of greater risk, instead of focusing on low-risk infrastructure.

3.2.1 RAMCAP Screening

Many RAMCAP sector modules will include a "top screen" to collect basic information to determine whether an asset is critical enough to warrant the performance of a more detailed RAMCAP assessment. However, in the Nuclear Sector, the "top screen" is not always necessary because some assets, such as commercial nuclear power plants, are all considered to be critical assets.

3.2.2 NRC Screening

The NRC is conducting SAs, in conjunction with PRAs that are described in section 3.2.2.1, across the range of sector assets to determine potential vulnerabilities and mitigative strategies for a range of threats against existing safety, safeguards, and security requirements, including security enhancements mandated since September 11, 2001. The assessments will allow NRC staff to confirm the adequacy of the existing regulatory framework, or form the basis for any changes that may be necessary, including such enhancements to address general and site-specific significant vulnerabilities identified through other NRC activities such as:

- Conducting force-on-force exercises at operating power reactors and Category I fuel cycle facilities to validate existing measures, or identify general or facility-specific vulnerabilities through the testing of actual performance

DRAFT

- Conducting inspections to validate existing measures, or identify general or facility-specific vulnerabilities
- Conducting tabletop exercises at operating power reactors and Category I fuel cycle facilities. Tabletop exercises are analytical tools used to give participants insight into the licensee's protective strategies. These exercises provide a detailed view of the protective strategies, including the support of the command structure, physical barriers, and personnel.
- Exploring the use of joint conflict and tactical simulation (JCATS), a computer simulation tool, to augment or replace tabletop exercises at operating power reactors and Category I fuel cycle facilities

The general approach to conducting SAs is through four basic elements, which can be used as screening analyses, detailed analyses, or both. These four elements are:

1. Threat characterization and scenario definition
2. Barrier analysis
3. Systems response analysis
4. Consequence analysis

These elements are not necessarily sequential, and results in one element can reduce or obviate the need for work in other elements. For example, if a threat or facility produces little or no consequences (consequence analysis screening), then further work on threat characterization, barrier analysis, and system responses is unnecessary. Several of the NRC's major security assessment efforts use this concept to great advantage. Some of the efforts described in later sections of this chapter, in regard to assessing consequences, vulnerabilities, and threats, are also used in this screening process.

DHS will complement existing SAs conducted by the NRC and licensees using the buffer zone protection plans (BZPP) template and training. The results will be used by the SSA, licensees, NRC, and State and local officials to develop effective strategies to enhance security around nuclear power plants and other sensitive nuclear facilities.

3.2.2.1 Screening during Licensing

As discussed earlier, part of the initial licensing process requires the applicant to submit a safety analysis report that includes a discussion of various hypothetical accident situations and their potential consequences. In addition, a probabilistic risk analysis (PRA) is applied as a systematic process for examining engineered systems design and operation based on these requirements and practices, and the manner in which human interactions with these systems work together to ensure plant safety. This process is quantitative, in that probabilities of events with potential public health and safety consequences are calculated, as are the magnitudes of these potential health consequences. The risk associated with such events is the product of the events' probabilities and their consequences. Information on this risk, and which failures contribute most to the risk, are of great value to the NRC and licensees in helping to determine the acceptability of a licensed facility's overall design and operation, as well as in focusing the NRC's and the regulated industry's resources on those aspects of design and operation that are most risk significant. The

DRAFT

NRC uses a decision-making framework process as a tool to aid in the evaluation of results of SAs into future security measures for materials and research and test reactor licensees. This tool assists in identification of the appropriate level of site-specific mitigative strategies required for given scenarios. The framework considers the attractiveness of the asset, system, or network and determines consequences based solely on prompt fatalities from radiation exposure and chemical effects associated with radioactive material processes.

To provide adequate protection of public health and safety, current regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power plants. A defense-in-depth philosophy is pursued in order to prevent accidents and to mitigate their consequences. Furthermore, emergency response provisions are mandated to provide additional defense-in-depth protection to the surrounding population in the unlikely event of an accident or event resulting in the release of radioactivity.

3.3 Assessing Consequences

Regardless of its initiator (e.g., terrorist act, human error, equipment malfunction, natural disaster, etc.), an event resulting in a significant radioactive release will have many potential consequences. Some of these consequences, such as acute radiation dose from a plume released from a nuclear power plant, or panic induced in the local population following the report of a terrorist attack on a nuclear facility, are prompt. Other consequences, such as those resulting from contamination of stored food supplies, contamination of local livestock and poultry, or long-term economic effects, are of a more chronic nature.

The discussion below describes the processes used by DHS to analyze the consequences of potential terrorist attacks across the various parts of the Nuclear Sector. The following areas are considered:

- Health Impact: Effect on human life and physical well-being (e.g., fatalities – both early fatalities and latent cancer fatalities, injuries)
- Governance Impact: Effect on the national Government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.
- Economic Impact: Effect on the local, State, Territorial, tribal, regional, or national economy (e.g., cost to rebuild asset, cost to respond to and recover from attack)
- Psychological Impact: Effect on the public's morale and confidence in the national economic and political institutions

DHS is working to examine consequences to other critical infrastructure and key resources through analysis of dependencies and interdependencies. One entity established in support of this effort is the National Infrastructure Simulation and Analysis Center (NISAC). NISAC's charter is to develop advanced modeling, simulation and analysis capabilities of the Nation's CI/KR and their physical and cyber cross-sector dependencies and interdependencies in an all-hazards context (natural, accidental, and malevolent). Table 3 in section 1.1.6 of this document details dependencies and interdependencies associated with the Nuclear Sector.

DRAFT

3.3.1 Assessment Methodology

The NRC and the nuclear industry employ several methodologies to assess the potential consequences that would occur if one of the industry's assets, systems, or networks was compromised. Security assessments (SAs) and safety assessments have been in use since the first civilian nuclear facilities were constructed in the 1960s. The NRC, with the support of National Laboratories, conducted extensive SAs in the 1970s and '80s. These assessments provided the foundation for the NRC's existing security requirements for power reactors and other facilities.

Following the September 11, 2001 attacks, the NRC initiated a series of SAs consisting of aircraft, land-based, waterborne, and cyber assessments to identify potential vulnerabilities of plant structures and systems, including reactor containments, spent fuel pools, and dry fuel storage casks. Security assessments are also being performed to identify potential vulnerabilities associated with radioactive material use, storage, and waste facilities. The results of the SA studies are used by the NRC to confirm and enhance, as necessary, the mitigative strategies put in place by the NRC's February 25, 2002 orders for a range of threats. These SAs support decisions by the NRC on whether existing security measures are sufficient to protect the public, and whether additional measures are necessary. The NRC incorporates the results of the SAs into any necessary regulatory improvements.

In late 2004, DHS, specifically the Risk Management Division (RMD), was given overall responsibility to coordinate and integrate the efforts of the different agencies in a Comprehensive Review (CR) of nuclear facilities. Multiple Federal organizations are required by various legislative and presidential mandates to conduct assessments of vulnerabilities, consequences, and responses for commercial nuclear power reactors and associated facilities to potential terrorist attacks. The CR process is intended to support the overall goal of reducing the nation's vulnerability to terrorism.

One of several CR teams will visit each of the nation's commercial nuclear power reactors and associated facilities over a projected two-year period that began in the spring of 2005. The individual assessments examine the site's exposure to attack, the consequences of such an attack, and the capabilities of local, State, and Federal to respond. The interaction between emergency response/preparedness and security is explicitly considered. The CR teams consist of representatives from DHS (RMD, CNPPD, USCG), FBI, NRC, and the industry. An analytical, logistical and administrative staff supports the CR field teams.

3.3.1.1 Regulatory Improvement

The NRC uses results from its ongoing security and mitigating measures assessments to assist in determining what, if any, additional preventive and mitigative actions may be needed to protect against threats that are likely to cause unacceptable consequences. Specific actions are required of licensees to protect against threats within the DBTs or pertinent threat characteristics, in cases where an applicable DBT has not been established. The NRC uses the results as the technical basis for subsequent actions and decisions regarding the design, operation, safety, and security of licensed facilities and activities. The results are also used to re-evaluate the physical protection, material control and accounting, access authorization, cyber security, safety and emergency preparedness controls, and related requirements needed for each category of facility and activity. Since September 11, 2001, the NRC has used these results to impose additional requirements on a wide range of licensees, as described elsewhere

in this document. Further regulatory improvements that the NRC may, for example, pursue after evaluating the results of an additional SA include:

- Working with licensees to assure well-implemented and well-executed mitigative or preventative measures
- Requiring immediate action to maintain safety or enhance security
- Modifying or eliminating current security measures
- Modifying the NRC's regulations and policies
- Issuing advisories, guidance, or other generic communications for significant, but not immediate, safety or security concerns
- Enhancing cyber security

At the same time, there is recognition that some threats to the sector are considered beyond what is reasonable to expect nuclear sector owner/operators of CI/KR, by themselves, to provide protective measures for, and the NRC will work closely with DHS and the private sector to address these threats.

The results of the SAs will also help to inform national decisions which support protecting the Nation's infrastructure.

3.3.2 Aircraft Attack at a Nuclear Power Plant

The Nuclear Sector believes that the prevention of an aircraft attack through such enhanced measures as airport passenger and baggage screening, strengthening of cockpit doors, and the Federal Air Marshal Program, remains the most effective strategy to protect our nation's infrastructure.

The NRC has conducted an extensive analysis of the potential vulnerability of nuclear power plants to aircraft attacks. While this analysis is classified, the NRC remains convinced that nuclear power plants are among the most heavily protected civilian facilities in the United States. SAs confirm that, in the event of a successful aircraft attack, the likelihood of damaging both the reactor core and releasing radioactivity that could affect public health and safety is low. Thus, the NRC maintains that nuclear power plant safety, security, and emergency planning programs continue to provide reasonable assurance of adequate protection of the public health and safety. The NRC continues to perform additional analyses to look for potential vulnerabilities and identify any appropriate mitigating actions. For example, the NRC is conducting structural analyses of two spent fuel pools to provide added assurance of spent fuel pool safety margin.

3.3.3 Assessing Emergency Planning in Determining Consequences

The intent of the NRC's emergency planning (EP) regulations is to reduce the impact of an accident on the public and the environment, and to protect the public from radiation exposure through protective actions that take into consideration plant conditions, evacuation times, shelter factors, and other conditions that may exist at the time of an event. The concept of emergency planning zones (EPZs) is discussed in detail in NUREG-0396, Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants. In essence, EPZs are areas for which detailed

DRAFT

pre-planning is required to assure that prompt and effective actions can be taken to protect the public in response to a radiological event. When considering the potential consequences of the impact of a release from a facility, it is useful to consider the area required for pre-planning as a means of distinguishing between the facilities. Appendix E to 10 CFR Part 50 addresses EPZs and emergency preparedness for production and utilization facilities. In Appendix E, NRC licensees are required to define EPZs surrounding their facilities, based upon the size of the reactor and the potential for the radioactive plume from a nuclear accident to affect the surrounding population. Appendix E divides the EPZ requirements into three areas:

1. Nuclear power plants with an authorized power level greater than 250 megawatts (MW) thermal—10 mile radius EPZ for plume exposure, 50 mile radius EPZ for ingestion exposure.

2. Gas-cooled nuclear reactors and nuclear reactors with an authorized power level less than 250 MW thermal—EPZ determined on a case-by-case basis (e.g. the now decommissioned Ft. St. Vrain's EPZ for plume exposure was 5 miles)

3. RTRs—EPZ requirements determined using NRC Regulatory Guide 2.6. (typically the EPZ for plume exposure is less than 1 mile)

The NRC continues to perform a post-September 11, 2001 review of security and the EP basis for nuclear power plants. The NRC has concluded that the EP basis for nuclear power plants remains valid in terms of timing and magnitude for the range of potential radiological consequences of a terrorist attack in the post-September 11, 2001 threat environment. Nuclear plant emergency plans in compliance with the EP basis provide reasonable assurance that adequate protective actions can be implemented to protect the public health and safety. This is true whether a reactor accident is caused by equipment failure, human error, natural phenomena, or terrorism. This assessment is based on multiple studies (some preliminary) performed by the NRC staff and its contractors.

3.3.4 Radiological Dispersal Device (RDD)

The use of radioactive materials in an unconventional attack via some dispersal mechanism, commonly known as a radiological dispersal device[23] (RDD), is widely recognized to have a greater likelihood of physical and social disruption than of lethal radiological consequences; however, the psychological and economic consequences of dispersal could be high. The consequences depend not only on the radioactive material involved (its isotopic composition and physical form), but also the dispersal mechanism (explosive or nonexplosive) and the environmental conditions under which it is released (e.g., urban, rural, weather). Thus, determining the absolute consequences of any potential dispersal in advance of its occurrence is impossible[24].

There is a wide range of possible consequences that may result from an RDD, depending on the type and size of the device, and how dispersal is achieved. The consequences of an RDD

[23] Radiological Dispersal Device (RDD)—A device or mechanism intended to spread radioactive material from the detonation of conventional explosives or other means.

[24] U.S. Department of Energy and U.S. Nuclear Regulatory Commission, "Radiological Dispersal Devices: An Initial Study to Identify Radioactive Materials of Greatest Concern and Approaches to Their Tracking, Tagging, and Disposition, May 2003.

may range from a small, localized area, such as a single building or city block, to large areas, conceivably many square miles; however, most experts agree that the likelihood of affecting a large area is very low. In most plausible scenarios, the radioactive material would not cause acutely harmful radiation doses, and the primary public health concern from those materials would be a small, more likely minute, increased chronic risk of cancer to exposed individuals.

3.3.5 Industrial and Medical Facilities That Use Risk-significant Radioactive Sources

The following discussion outlines the manner in which the NRC, DOE, and IAEA use potential radiological consequences to set thresholds for tracking radiological material.

In June 2002, the Secretary of Energy and the Chairman of the NRC convened an Interagency Working Group on RDDs to address the Nation's concerns regarding the use of radioactive materials for a malevolent act. The Working Group's report[25] used a systematic analysis to broadly assess radioactive materials and determine which are of greatest concern for use in an RDD. The report used input from an analysis prepared for this purpose by Sandia National Laboratories[26] to provide a relative indication of materials of concern, rather than an absolute ranking. The report identified those radioactive materials of greatest concern, which were given first priority for consideration of increased security measures.

Concurrently, the IAEA, in developing the revision of the Code of Conduct for the Safety and Security of Radioactive Sources, assessed the relative risk of sources in TECDOC-1344[27]. This TECDOC publication provides a categorization system for ranking radioactive sources based on their potential to cause harm to human health, and for grouping the practices in which these sources are used into discrete categories. The purpose of categorizing radioactive sources is to provide a fundamental and internationally harmonized basis for risk-informed decisions. It provides a categorization for radioactive sources used in industry, medicine, agriculture, research and education.

Consistent with the NRC's overall approach, SAs are being performed for licensed users that possess risk-significant quantities of radioactive material. Because of the great number and diversity among users, representative facilities with radioactive materials in quantities of concern are being assessed.

3.3.6 Radioactive Material Transportation Packages, and Radioactive Waste and Storage

The SA methodologies for radioactive material transportation packages, and radioactive waste and storage of the sector are discussed below. Significant protective measures continue to ensure the safe transport of such risk-significant nuclear material as special nuclear material and high-level waste. It is unlikely that a significant release of radioactivity would occur from an accident involving the transport of this type of material. However, any release resulting from a terrorist or malevolent act would, in all likelihood, be localized, which would limit the potential

[25] Ibid

[26] Sandia National Laboratories, An Initial Study to Identify Materials of Greatest Concern for Use in a Radiological Dispersal Device, November 15, 2002.

[27] International Atomic Energy Agency, Categorization of Radioactive Sources, TECDOC-1344, Revision of IAEA-TECDOC-1191, Categorization of radiation sources, July 2003.

consequences on the public. Any material stolen or diverted from a shipment could, however, be used in an RDD, with similar potential consequences to those described above.

Current regulations ensure adequate protection of the public and the environment from radioactivity remaining at a reactor site when the reactor license is terminated following decommissioning. Consistent with the safety requirements at decommissioned sites, the NRC will consider on a case-by-case basis reducing the requirements for emergency planning, onsite and offsite insurance, and safeguards for permanently shut down-plants as requested by licensees.

Spent fuel storage casks are maintained at several decommissioned sites. These casks present a possible target for terrorists who may attempt to carry out an aircraft attack. Another possible method of attack on spent fuel storage casks is an explosive detonation adjacent to a cask. The NRC has sponsored scientific studies to investigate the results of both scenarios from the perspective of initial impact from the aircraft/explosion, and the subsequent fire that would result. The results of these studies are classified. In 2002, the NRC required enhancements to security measures for spent fuel storage in pools and in dry storage casks.

3.3.7 Research and Test Reactors

The NRC is nearing completion of a comprehensive decision-making framework process that uses SA information to determine the appropriate level of mitigative strategies to be implemented at RTRs. For these detailed SAs, specific threshold scenarios, action sequences, and adversarial attributes were developed. The NRC will use the detailed SAs to determine whether any actions are required by the affected licensees. In the interim, the NRC has worked with licensees who own and operate RTRs to enhance security measures. The NRC confirmed the measures were established through the issuance of confirmatory action letters and subsequent inspections. In addition, the NRC has worked with the licensees to develop specific protective measures graded for threat levels to implement the Homeland Security Advisory System (HSAS). More information on the decision-making framework can be found in section 3.4.1.

3.3.8 Other Industrial and Medical Facilities

There are other facilities that use radioactive materials that are not categorized as radioactive materials in quantities of concern. The form and quantity of material varies greatly, ranging from small tracer amounts of radiochemicals to large quantities of unsealed materials utilized in radiopharmaceutical, radiochemical, or risk-significant sealed source manufacturing. The license for these facilities may contain certain conditions imposed by the NRC or Agreement State, and agreed to by the licensee, that takes into account emergency preparedness and response plans commensurate with the scope of operations and the potential risk posed by the materials the licensee is authorized to possess. Users of radioactive material that pose a greater risk to workers or the public are required to be analyzed in greater detail and some may be required to have a formal emergency plan subject to approval by the NRC or Agreement State. Some may also be subject to NRC orders for enhanced security measures in addition to regulations and license conditions for securing radioactive materials.

DRAFT

3.3.9 Tools for Assessing the Consequences of a Radiological Event

Considerable insight into the consequences of a radiological event can be gained by using computer modeling software. Generally, the software takes into account the source term, or amount of radiation associated with the release, and factors in the atmospheric conditions in the vicinity of the release, to model the exposure to the surrounding public caused by the radioactive plume.

An example of a modeling program is the Radiological Assessment System for Consequence Analysis (RASCAL) program, which projects radiological consequences during accidents that can be compared to EPA protective action guidance and thresholds for acute health effects. The NRC is enhancing the code with a new RDD source term library that incorporates results from Research and Development (R&D) testing of mock RDDs. The RASCAL-generated source terms are used by the National Atmospheric Release Advisory Center (NARAC) in atmospheric dispersion codes. Also, RASCAL-generated deposition patterns are used by the Federal Radiological Monitoring and Assessment Center (FRMAC) for initial assessments of nuclides present and doses from deposited materials.

The October 2004 Nuclear/Radiological Incident Annex of the National Response Plan states that, for Incidents of National Significance, "The Interagency Modeling and Atmospheric Assessment Center (IMAAC) is responsible for production, coordination, and dissemination of consequence predictions for an airborne hazardous material release. The IMAAC generates the single Federal prediction of atmospheric dispersions and their consequences utilizing the best available resources from the Federal government." In November 2004, the NRC approved a memorandum of agreement with IMAAC on the roles and responsibilities of Federal departments and agencies with respect to IMAAC.

3.4 Assessing Vulnerabilities

3.4.1 Engineering Analysis of Nuclear Facility Vulnerabilities

As previously described, the NRC uses a risk-informed approach to assessing vulnerabilities of licensed nuclear facilities and radioactive materials. A SA is a systematic evaluation in which qualitative and quantitative techniques are applied to determine potential vulnerabilities to radiological sabotage or theft or diversion of radioactive material. The NRC uses SAs to identify effective countermeasures and mitigating measures that can be used to protect specific targets or materials. The results are used by the NRC to confirm or enhance the mitigating measures implemented as a result of the February 25, 2002 NRC orders and to assist national efforts to enhance infrastructure protection.

The NRC conducted SAs for operating power reactors, spent fuel pools, nuclear fuel cycle facilities, transportation of nuclear material, and radioactive sources in the 1970s and 1980s. These assessments were used to establish the technical basis for security requirements for the facilities and materials. The potential impacts of terrorist attacks on power reactors were also routinely evaluated as part of the Force-on-Force exercise program on a plant-by-plant basis during the 1980s and 1990s. Force-on-Force exercises are also conducted at Category I fuel cycle facilities in accordance with 10 CFR 73.49 (9). The NRC observes one exercise at the Category I facilities annually. In addition, as a result of growing concerns about the threat and vulnerability of critical facilities to computer attacks, the NRC initiated cyber SAs in 1991. Prior to 2001, there were no SAs of an intentional aircraft attack on a nuclear power plant, although

DRAFT

some evaluations had been conducted to assess accidental crashes and the loss of large areas of the plants due to natural disasters, fires, or explosions.

After the terrorist attacks in 2001, the NRC promptly assessed the likelihood and potential consequences of terrorists targeting nuclear facilities for air attack, the physical effects of such a strike, and such compounding factors as meteorology that would affect the impact of potential radioactive releases beyond the site boundary. As a result of these preliminary evaluations, the NRC required that nuclear power plant licensees conduct interim enhancements to mitigate potential consequences in the unlikely event of a successful air attack on a nuclear power plant.

The NRC also initiated a series of SAs consisting of aircraft, waterborne, ground, explosive, and cyber assessments to identify potential vulnerabilities of plant structures and systems. As for the potential for aircraft impact, the NRC has evaluated the "hittability" and potential consequences of an aircraft attack on nuclear power reactors, considering site layout, systems design, topographical features, and mitigation systems. Of primary importance is the design of the nuclear power plants themselves. Although nuclear power plants were not specifically designed to resist attack by aircraft, such as those that struck the World Trade Center and Pentagon, nuclear power plant structures are extremely robust, and provide strong barriers that would help to limit the effects of an aircraft strike. Nuclear power plant structures also have relatively low profiles, and many are shielded by natural or man-made obstacles such as hills, trees, power lines, and other buildings, reducing the likelihood of a successful hit by an aircraft.

With respect to waterborne threats, the NRC has collaborated with the U.S. Coast Guard (USCG) regarding the assessments required under the Maritime Transportation Security Act. The NRC has established interaction with the USCG in the development of area maritime security plans, participated in the Coast Guard Underwater Assault Working Group, and is developing an agreement with the USCG in this area. The NRC has conducted specific studies of potential nuclear power plant vulnerabilities to attacks from the bodies of water located adjacent to the plants. NRC's April 2003 DBT orders require nuclear power plants to defend against waterborne assaults.

In January 2005, the NRC initiated implementation of a decision-making process (framework) for materials and RTR SAs. This decision-making framework serves as a tool for NRC to use SA information to determine the appropriate level of mitigative strategies required for a given threat scenario for specific materials or RTRs. The development of the decision-making framework was informed by the DHS Risk Analysis and Management of Critical Assets Protection (RAMCAP) methodology. The facility-specific description which was used as part of the SA input to the decision-making framework was provided to respective individual licensees for verification. Framework results, in conjunction with facility-specific SAs and reviews, which focus on prompt fatalities, are used in the determination of whether further actions by NRC are necessary to enhance facility security and/or measures to mitigate the consequences resulting from an attack.

Further NRC SA efforts will be directed to confirm and extrapolate results of existing studies. Studies will focus on power reactor facilities and spent fuel pools to identify the consequences and risk mitigation measures associated with specific modes of attack. The NRC is developing SA methodologies to examine specific elements of the current threat environment.

DRAFT

3.4.2 Radioactive Material Users and Sources (Radioactive Materials in Quantities of Concern)

Facility vulnerabilities are determined using a performance-based approach to assess the physical security protection system effectiveness for preventing theft and sabotage events. Site visits to the representative facilities provide site-specific data, along with expert judgment in assessing physical protection system effectiveness. A conditional probability of successful attack is calculated for a variety of event scenarios using an adversary threat matrix with increasing capabilities. Facilities are analyzed at the path and scenario levels. The relative probability of successful attack is used to categorize the event threat scenarios. Risk is then evaluated qualitatively, using a risk matrix, by integrating the consequences for each scenario with the conditional probability of successful attack. Risk rankings by facility, type of material, event, scenario, and threat, are developed. The lowest adversary levels were determined to be the realistic threats for which to begin identifying countermeasures.

The materials SA also evaluates cyber systems and human element vulnerabilities. The human element is considered in both the physical protection system and in the adversary threat matrix (e.g., insider threat). Generally, information technology/cyber system elements do not control chemical/physical processes involving radioactive materials in quantities of concern whose failure would result in a consequence of concern. Rather, cyber system elements are assessed consistent with their importance to the physical protection system (e.g., access controls) and its effectiveness for preventing a theft or sabotage event.

Countermeasures for reducing the consequences and improving the physical security protection system effectiveness are evaluated. Inventory reduction, and limiting facilities to specific forms and quantities of isotopes are considered for reducing the consequences of events. Countermeasures to improve the probability that adversaries will be detected, interrupted, and successfully neutralized are assessed. General cost information is developed for countermeasures to examine the tradeoff between cost and the risk-reduction benefit.

3.4.3 Transportation of Risk-significant Radioactive Sources

Prior to September 11, 2001, the most probable event to produce undesirable consequences for radioactive material shipments was thought to be a severe accident on a roadway, waterway, railway, or in the air. In today's threat environment, the possibility that a shipment may be stolen, attacked, or diverted for malicious purposes must also be considered.

In the aftermath of the terrorist attacks of September 11, 2001, the NRC issued multiple safeguards advisories to enhance the security of spent fuel transportation and shipments of Radiological Material Quantities of Concern (RAMQC). These advisories recommended that licensees implement additional security measures during shipments; licensees fully adhered to these advisories. The NRC also required enhancements for security measures for spent fuel shipments from power reactors and RTRs beginning in August 2002. The security measures for shipments have also been adjusted to reflect changes in the Homeland Security Advisory System (HSAS) threat level.

In addition to the safeguards advisories, the NRC has used regulatory issue summaries (RISs) as a method to provide guidance on such subjects as:

- NRC Threat Advisory and Protective Measures System

DRAFT

- Additional protective measures for transportation of spent nuclear fuel (SNF) greater than 100 grams
- Use of existing emergency plans and procedures for the potential deployment of National Guard, State Police, and other emergency responders in the controlled and unrestricted areas at a nuclear power plant
- Filing requirements for advance notification of the shipments of SNF and SNM

Additionally, the Homeland Security Act of 2002 amended the Federal hazardous materials transportation law, 49 USC 5103, to include security in the Secretary of Transportation's mandate to "prescribe regulations for the safe transportation, including security, of hazardous materials in intrastate, interstate, and foreign commerce." DOT's Pipeline and Hazardous Materials Safety Administration issued regulations effective September 25, 2003 requiring shippers and carriers of most hazardous materials, including certain radioactive materials, to develop and implement security plans and to ensure that their employee training includes a security component. The security plans are based on a structured analysis, such as DOT's Risk Management Self-Evaluation Framework (RMSEF), and cover personnel security, unauthorized access, and en-route security. The DOT's Federal Motor's Carrier Administration issued also regulations effective January 1, 2005 requiring safety permits for a highway route controlled quantity of radioactive material (HRCQ), which included having a satisfactory security program and associated training.

The radioactive material shipment process is, by nature, not particularly dependent upon cyber system inputs, and therefore, is not susceptible to cyber intrusions. While generic route notifications are made to the NRC via normal telecommunications links for shipments of consequence, the information is of a time-sensitive nature, and shipping packages are well-protected under NRC, DOE and DOT regulations. Additional security measures have been implemented via NRC orders for RAMQC notifications made by licensees. Routes and times for spent fuel shipments are protected as Safeguards Information, and sent to the NRC via noncyber-related media.

The NRC has also supported efforts by the DHS Bureau of Customs and Border Protection (CBP) and the USCG to begin advance electronic notifications of dangerous goods crossing United States borders, and to implement regulations on port and facility security.

In parallel with these enhancements, the NRC is assessing the potential vulnerabilities and mitigating strategies for a spent fuel rail transport package design, a spent fuel truck package design, and three radioactive material package designs. The NRC evaluated the response of the packages to ground assault tactics consistent with the radiological sabotage DBT, including a range of explosive threats.

3.5 Assessing Threats

The threat in the Nuclear Reactors, Materials, and Waste Sector can be broadly categorized into three classes: (1) threats of radiological sabotage; (2) threats of a malicious or terrorist act that uses radioactive material or special nuclear material stolen or diverted from a nuclear facility; and (3) threats of an intrusion into the cyber systems at a nuclear facility.

DRAFT

The DHS, NRC, and other Agencies have concluded that a general credible threat of attacks exists on nuclear facilities and of theft of risk-significant radioactive material. This threat is larger than assumed prior to September 11, 2001.

NRC requirements in 10 CFR Part 73.1 (a) and related security orders, describe the design basis threats (DBTs) that apply to nuclear power reactors and Category 1 special nuclear material (greater than a formula quantity of strategic special nuclear material). These DBTs have been substantially increased following September 11, 2001. For the remainder of facilities that are not required to have a DBT, the NRC gathers and provides information on the spectrum of threats, and ensures the continued adequacy of security measures to protect against these threats. This information provides a consistent basis for SAs and security measures.

The Nuclear Regulatory Commission (NRC) has proposed to amend its regulations that govern the requirements pertaining to design basis threat (DBT). The proposed rule would amend the Commission's regulations to, among other things, make generically applicable the security requirements previously imposed by the Commission's April 29, 2003 DBT orders, which applied to existing licensees, and redefine the level of security requirements necessary to ensure that the public health and safety and common defense and security are adequately protected. The proposed rule would revise the DBT requirements for radiological sabotage (applied to power reactors and Category I fuel cycle facilities), and theft or diversion of NRC-licensed Strategic Special Nuclear Material (SSNM) (applied to Category I fuel cycle facilities). The NRC has developed draft Regulatory Guides (RGs) that provide guidance to licensees concerning the DBT for radiological sabotage and theft and diversion. These draft RGs have limited distribution because they contain either SGI or classified information. The specific details related to the threat, which contain both SGI and classified information, are contained in adversary characteristics documents (ACDs) that are not publicly available. These documents include specific details of the attributes of the threat consistent with the requirements imposed in the April 29, 2003, DBT orders.

The NRC, in concert with DHS/SSA and the intelligence and law enforcement communities, evaluates the current threat environment affecting regulated activities, and performs rapid assessment of the credibility of threats and security events. In addition, the NRC formally reviews the threat environment semiannually as part of a review of the adequacy of NRC's DBTs based on domestic and foreign events, and intelligence information. This process provides critical information that forms the basis for updates to the DBTs (most recently in April 2003). After performing a peer review with DHS/SSA and other cleared stakeholders, the NRC staff proposes updates to the DBTs to the NRC's Commission, if necessary. Participation in these assessments are important in that security partners can understand the risks to their facilities and make educated decisions on protective measures to enact. Also, information sharing will result in better identification of risks and vulnerabilities, which helps industry partner with others to protect its key assets, systems, networks, and functions.

Compiling, evaluating, and protecting threat information is pivotal to the NRC's ability to assess and define the threat environment. Since September 11, 2001, NRC-licensed facilities have been reporting incidents of a suspicious nature to the NRC Operations Center and regional offices. These reports comply with requests made by the NRC in a series of advisories following September 11, 2001. The NRC maintains this information in a protected Web server and database that are shared with authorized users. A descriptive report is filed each time a licensee calls in a security-related event, along with information shared with other licensees, and local, State, or Federal agencies. The database allows the NRC's Threat Assessment

DRAFT

Section to evaluate the number and types of events, search for any adverse trends, and share security information with homeland security, law enforcement, and licensee officials who have a need to know. Information on how DHS protects business sensitive or proprietary information can be found in Section 2.5.

3.5.1 Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

Periodic Nuclear Sector-wide risk assessments are performed by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) division within DHS. HITRAC's vision is to be the pre-eminent National center for the integration, analysis, and sharing of information regarding the risks of terrorist attacks to U.S. infrastructure for others in DHS, other Federal Departments and agencies, the Intelligence Community (IC), State and local governments and law enforcement agencies, and the private sector.

Tactically, HITRAC evaluates and monitors current threat to U.S. infrastructure, and support DHS decision makers and external customers with immediate analysis. Strategically, HITRAC maintains situational awareness of infrastructure sectors and develops long-term strategic assessments of their risk factors. This is done by integrating threat information with the unique vulnerabilities and consequences of an attack associated with each infrastructure sector.

HITRAC has briefed government and private sector stakeholders in the Nuclear Sector on the sector's threat information, and will continue to do so.

In a HITRAC threat brief, information is provided such as: the brief's key findings; a threat overview, including an introduction, threat themes, and other reporting not associated with a particular threat theme; sector vulnerabilities; scenarios of concern; consequence overview; actions to reduce risk; and point of contact information.

3.6 Challenges

3.6.1 Cyber

Cyber Vulnerability. New domestic and international adversaries are emerging, and new tools are appearing that can be used by adversaries to exploit vulnerable systems. The NRC and the nuclear industry are faced with the growing challenge of protecting nuclear facilities from cyber threats that could impact safety, security, and emergency response at nuclear facilities.

3.6.2 Physical

The events of September 11, 2001 forced the Nuclear Sector to review the adequacy of security measures for a broad range of licensees against a broad range of threats. The challenge lies in ensuring that the level of protection of nuclear facilities and materials remains adequate in a dynamic threat environment, and in a manner that minimizes unnecessary regulatory burden and maximizes stability of the regulatory framework.

Risk Harmonization. Nuclear facilities remain secure, and have enhanced security following the September 11, 2001 attacks. When compared to other CI/KR facilities and assets, nuclear facilities are more secure. The challenge is to allocate security resources to reduce risks, to the homeland and avoid squandering resources on lower risks to the detriment of public safety.

DRAFT

3.7 Initiatives

Cyber Vulnerability. (See section 3.1.3)

Security assessments. Further NRC SA efforts will be directed to confirm and extrapolate SA results. Studies will focus on power reactor facilities and spent fuel pools to identify the consequences and risk mitigation measures associated with specific attacks. Development of land-based assault SA methodologies is also planned for use by NRC and licensee security staff to design more sophisticated physical protection systems than those in place today. Blast effect engineering studies will provide a methodology to assess the fragility of structures, and will be used by licensees when performing blast-effect analyses.

Since the 1980s, the NRC has regularly carried out force-on-force exercises at operating nuclear power plants. Force-on-force exercises are conducted to assess vulnerabilities and improve, as necessary, the performance of defensive strategies at licensed facilities. These exercises have been, and are intended to be, a primary means to conduct performance-based testing of a licensee's security force and its ability to prevent radiological sabotage as required by NRC regulations (10 CFR Part 73).

Legislation. Over time, the NRC has proposed legislation to the Congress that would allow the NRC's Commission to enhance nuclear security. Legislation proposed by the NRC, and coordinated with the DHS/SSA and the Administration, includes provisions that are important to the protection of the Nation's civilian nuclear infrastructure, and that would help to prevent the use of risk-significant radioactive sources as radiological weapons (RDDs and radiological exposure devices [REDs]).

The most important nuclear security enhancements proposed by the NRC, and incorporated in the Energy Policy Act of 2005, include the following:

- Authorization of security personnel at NRC-regulated facilities and activities to receive, possess, and, in appropriate circumstances, use more powerful weapons important to defending against terrorist attacks
- Enlargement of the classes of NRC-regulated entities and activities whose employees are subject to fingerprinting and criminal history background checks
- Federal criminalization of unauthorized introduction of dangerous weapons into nuclear facilities
- Federal criminalization of sabotage of additional classes of nuclear facilities, nuclear fuel, and radioactive material
- Authorization for the NRC to carry out training and fellowship programs to address shortages of individuals with critical nuclear safety regulatory skills
- Extension of the NRC's regulatory authority to include discrete sources of accelerator-produced radioactive material and radium-226, which are not currently covered by the Atomic Energy Act
- Requirement for the NRC to consult with DHS concerning the potential vulnerabilities of the location of a proposed facility to terrorist attack prior to issuing a license for a utilization facility. This process is currently under development.

DRAFT

Radioactive Material Users and Sources (risk-significant radioactive material). Since shortly after the terrorist attacks in 2001, the NRC has been working with States and licensees to enhance the security and control of risk-significant radioactive materials. These efforts have included identifying materials of highest risk from a security perspective, and enhancing the security and safety of these risk-significant materials. Licensees who possess risk-significant materials are now implementing increased controls, and the NRC and Agreement States are verifying the adequacy of implementation through inspection. Additional security measures are also being considered for other material.

As explained in the previous section on prioritizing assets, the NRC first enhanced controls on panoramic irradiators, and manufacturers and distributors of radioactive sources. These enhancements are now in place, and have been inspected by the NRC or Agreement State inspectors under agreements with the NRC.

The NRC and Agreement States are continuing with these enhancements by addressing additional licensees with radioactive materials in quantities of concern and IAEA category 3 and beyond (in aggregate). Increased controls are being required for groups of radioactive material users that include industrial, medical, or research irradiators, medical teletherapy, industrial radiography, well logging, and industrial gauges. Issuance of the increased controls for licensees in IAEA categories 1, 2 and 3 and beyond (when aggregated) is complete. NRC and the Agreement States, under the authority to protect the public health and safety and the environment, are in process of issuing legally binding requirements to put essentially identical increased controls in place for licensees under their regulatory jurisdiction. Licensees will complete their implementation of these enhancements by June 2006. Then, NRC and the Agreement States will inspect licensees' compliance with the increased controls.

Industry Initiatives. The nuclear industry, under the auspices of NEI, has contracted the Electric Power Research Institute (EPRI) to perform several proprietary activities regarding security issues related to the industry. Several of the EPRI efforts are ongoing, including aircraft impact studies of nuclear power plants. Additionally, the following reports have been developed by EPRI, either for or related to the Nuclear Sector:

- Probabilistic Consequence Analysis of Security Threats—A Prototype Vulnerability Assessment Process for Nuclear Power Plants, Report # 1007975, April 2004
- Supervisor Control and Data Acquisition (SCADA) Systems Security Guide, Report #1002604, November 2003
- An Approach to Risk-Informed Changes to Physical Security, Report # TR-113787, October 1999

Federal Initiatives. The NRC has been working with DHS, DOE, the FBI, DOT, DOS, the IAEA, and others to enhance physical protection and control of sources of radioactive material that present the highest risk if used by a terrorist in an RDD. Elements of cradle-to-grave security enhancements will include:

- Verification of the legitimacy of applicants for licenses to use radioactive material
- Requirements governing the shipment, storage, and use of radioactive material in quantities of concern
- Controls on access to radioactive sources to prevent diversion by an insider

DRAFT

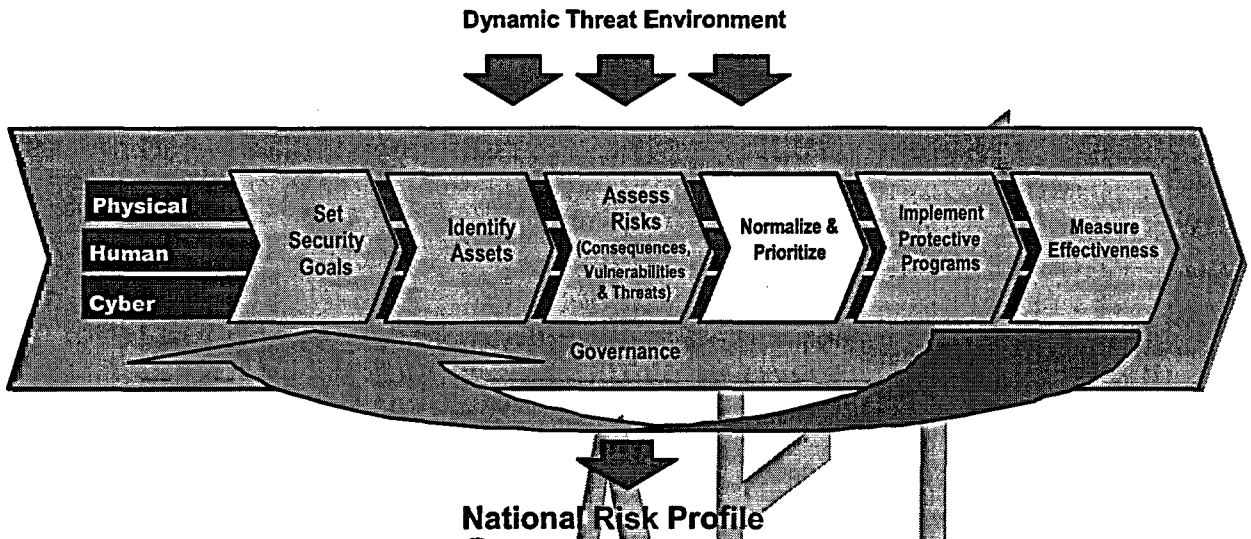
- Tracking and inventorying radioactive material in quantities of concern to ensure that they have not been lost or stolen
- Export and import controls on radioactive material in quantities of concern

Working with State radiation control programs, the NRC has required certain materials licensees to enhance security for panoramic irradiators (June 2003), and manufacturers and distributors that possess radioactive materials in quantities of concern (January 2004) to reduce or mitigate potential security vulnerabilities. To help guide these efforts and develop security enhancements in a cooperative manner with the States, the NRC, the Conference of Radiation Control Program Directors (CRCPD), and the Organization of Agreement States established the Materials Security Working Group and the Materials Security Steering Committee to guide the efforts of the working group in June 2003. The working group and steering committee have been instrumental in developing the performance elements (also known as additional security measures [ASMs] and increased controls) for security enhancements for NRC and Agreement State licensees possessing or using risk-significant radioactive materials used in industrial, medical, and academic applications. The NRC has also issued a final rule that enhances the security of small portable gauges that contain radioactive material, but do not exceed the risk-significant threshold.

Risk Harmonization. Several of the initiatives discussed under physical security also address the challenge of risk harmonization. An example is the Federal and industry effort to identify the most radioactive materials in quantities of concern possessed by licensees, and develop a method to accurately keep track of them. In addition, the cyber security initiative represents a focused and well-thought-out effort to protect cyber vulnerabilities in the sector.

DRAFT

4 Prioritize Infrastructure



4.1 Process to Prioritize Infrastructure

Even with all of the resources of the United States, it is not possible to protect every asset against every possible type of terrorist attack. Consequently, the Nation's CIP program must prioritize protection across sectors, so that resources are applied where they offer the most benefit for reducing risk by deterring threats, reducing vulnerabilities, and minimizing consequences of attacks. For instance, nuclear power plants are among the most well defended and robust commercial installations in the United States. They are constructed to maintain a high degree of safety in the event of natural disasters such as hurricanes and tornadoes as well as equipment malfunction or damage. They also have large and highly trained guard forces.

Using a systematic and consistent way of prioritizing assets offers transparency and increases the defensibility of the decisions that are made about both government and private sector resource allocation. Similar principles apply within individual CI/KR sectors as well, and CIP efforts must be prioritized within the Nuclear Sector to maximize the benefits of the limited CIP resources specifically dedicated to the Nuclear Sector. This chapter of the document addresses the process used to normalize the results of assessments of nuclear facilities, and prioritize the sector's assets, systems, networks, and functions. Federal government's support given to protective efforts within the Nuclear Sector is based on those results.

There will also be a prioritization among the all of the CI/KR sectors, including the Nuclear Sector. However, that prioritization is addressed in the NIPP base plan, and is not discussed here. Still, the prioritization that occurs within the Nuclear Sector assists in the overall prioritization across all the CI/KR sectors.

4.1.1 DHS Efforts to Prioritize Infrastructure

As described in the preceding section, the ultimate goal of RAMCAP is the development of a risk assessment methodology that would allow DHS to compare the risk of an asset to the risk associated with other similar assets as well as assets from different sectors. Using the widely-accepted risk equation wherein an asset's risk is a function of the likely consequences of a successful attack, the asset's vulnerability to attack, and the likelihood of an attack on the asset, DHS is able to determine a numerical risk score for an asset.

When comparing risk, risk scores can also factor in the known inter- and intra-sector dependencies and interdependencies. Those dependencies and interdependencies are detailed in section 1.1.6. Some of the most critical dependencies include connections with the energy sector based on the electricity that nuclear power plants provide the electric grid and the public health/healthcare sector as the Nuclear Sector provides many items to the medical community, including pharmaceuticals and diagnostic substances. Also, if other CI/KR is within close physical proximity of a Nuclear Sector asset, the potential radiation release from the Nuclear Sector asset could impact the nearby CI/KR. Efforts to understand dependencies and interdependencies in greater detail than they are today, which will assist with the prioritization effort, are covered under Goal #2.

As risk scores are determined for multiple assets, those assets can be prioritized based on their risk.

Phase II of the RAMCAP effort, which is currently underway, involves the development of sector- or sub-sector-specific modules to assist in implementation of this asset prioritization. Included in these modules will be sector-specific risk-assessment (RA) guidance documents to assist asset owner/operators in determining vulnerabilities and consequences in a format that allows determination of an ultimate risk score that can be compared with risk scores for assets from other parts of the Nuclear Sector that do not currently utilize RAMCAP.

DHS and ASME are cognizant of the fact that numerous consequence, vulnerability, and risk assessment methodologies were in existence and being employed by various parts of the Nuclear Sector prior to the development of RAMCAP. The risk assessment methodology being developed as part of the Nuclear Sector RAMCAP module will be able to use the results from various other methodologies already in use in the sector, and will be able to normalize the data compiled using those other methodologies to allow for prioritization of assets based on risk, as is required to optimize resource allocation decisions.

CNPPD, as the SSA, along with the NRC and the rest of the GCC, has the responsibility to prioritize the assets in the Nuclear Sector. This effort will continue to be refined as time goes on. Sometimes, the prioritization can be as specific as a ranked list. Other times, having a few different categories of relatively higher and lower risk, and placing all assets into one of those categories, is all that is needed. Physical and cyber assets are both considered during the prioritization process, although there currently has been more detailed prioritization that has occurred with the physical assets. Cyber assets, to this point, have generally been placed in one of the broader categories of relatively higher or lower risk. These prioritization efforts will occur on an as needed basis, recognizing the benefit that prioritization has informing the decision making process used to implement protective measures.

DRAFT

DHS maintains the National Asset Database (NADB) as mentioned in Section 2.1. While the NADB is not a prioritized list of the Nation's critical infrastructure, the data contained therein is searchable in a variety of ways, and can be used to create prioritized lists based on selected parameters.

There is also recognition that decisions on risk assessments can be controversial, reflecting the important role that both science and judgment play in drawing conclusions about threat, vulnerability and consequence, as difficulty exists in fully quantifying the three components that comprise risk. Perceptions can vary based upon such factors as the extent to which the stakeholders are directly affected, whether they have voluntarily assumed the risk or had the risk imposed on them, and whether they are connected with the cause of the risk. DHS considers these factors when making prioritizations based upon risk.

4.1.2 Other Sector Efforts to Prioritize Infrastructure

Following September 11, 2001, the NRC prioritized assets based on the potential consequences of a successful attack. The subsequent sequences of regulatory actions taken by the NRC reflect a higher-order set of priorities from a security perspective. This is also reflected in the NRC's implementation of the HSAS.

The NRC used the results of the SAs to develop and issue RISs to each of the categories of licensees listed above. These RISs contained security measures corresponding to each of the five color-coded levels contained in the HSAS.

The NRC is also using the SA results and coordinating with licensees, the SSA, and other Federal and State agencies to continue to develop necessary enhancements to security measures to protect the public safety. These additional enhancements are expected to be applied to the transportation of RAMQC (other than spent fuel and Category 1 quantities of strategic special nuclear material) and other uses of radioactive materials in quantities of concern.

4.1.2.1 Materials Licensees

As discussed in section 4.2.5 Analysis of Consequences, the IAEA has categorized radioactive sources based on their potential to cause severe deterministic health effects.

The NSCC-Radioisotopes Subgroup has developed an inventory of applications used beyond the scope of nuclear power, fuel cycle, nonpower reactors and waste facilities. The list of applications was compiled from information available from NEI, industry groups and representatives of companies or users from this vast community. The inventory was then used as the basis of a matrix that for each category of use provides a description of use, form of materials used, typical radionuclides and maximum quantity. The matrix was developed for the purpose of ensuring that the wide range of radioactive materials applications beyond the scope of nuclear power, fuel cycle, nonpower reactors and waste facilities in the Nuclear Sector were represented as assets and for consideration on the basis of risk for additional controls to protect this sector of the infrastructure. While not all applications involve the use of radioactive materials in quantities of concern, those that do have been highlighted in accordance with the IAEA categorized approach and given priority status on this basis of risk. The matrix has been provided to the NRC and was found to be consistent with their risk assessment, also based on the IAEA Code of Conduct categorization.

DRAFT

4.1.2.2 Radioactive Materials Shipments

Shipments of radioactive materials are categorized based on the amount of each isotope contained in the shipment. Any shipments of amounts above a given threshold are reported to the NRC Operations Center. The shipper must provide the amount and type of material shipped, departure and arrival dates and locations, and the route and mode of travel, for each leg of the shipment. Consistent with the NRC's orders on RAMQC shipments, other security precautions are also undertaken, such as pre-notification of States through which shipments are made. Federal regulations define the requirements for shipping radioactive material. Shipments are prioritized based on the amount of each type of isotope in the shipment.

Spent fuel shipments, and shipments of strategic special nuclear material, are given a higher priority than are other radioactive materials due to serious potential consequences should a shipment be compromised. Shipment times and routes are sent to the NRC Operations Center. Certain information related to the shipments is protected from disclosure or controlled as Safeguards Information. Extra precautions include obtaining NRC approval for a shipping plan, minimizing time and transit, avoiding intermediate stops, armed escorts, immobilization devices, and notifying State Governors' representatives of the shipments.

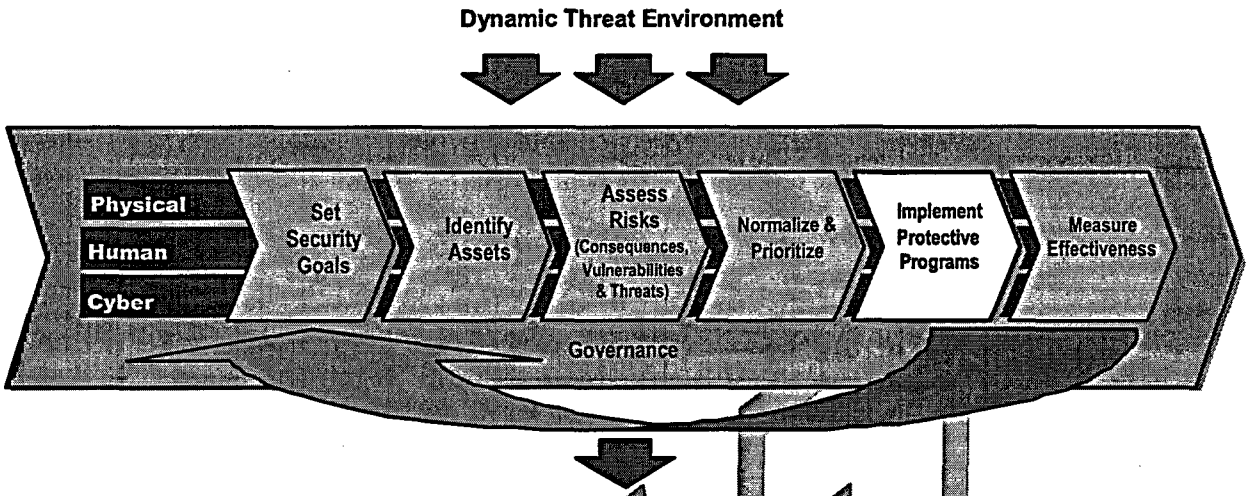
Shipments of radioactive materials in quantities of concern or radionuclides of concern are also reported and tracked, to maintain situational awareness and coordinate actions in response to threat information and security plans.

4.1.2.3 Radioactive Waste Facilities

Spent fuel storage facilities, along with power reactor facilities, and other facilities that possess radioactive materials in quantities of concern are prioritized based on the size and type of source material. Other types of radioactive waste facilities (e.g., low-level waste storage/disposal and uranium mills) are not expected to pose significant offsite consequences in the event of an attack.

DRAFT

5 Develop and Implement Protective Programs



The minimum required security posture for commercial nuclear power plants and Category 1 special nuclear material that is the responsibility of the owner/operator is defined by NRC regulation, based upon the design basis threat (DBT). The DBT elements and characteristics represent the largest spectrum of threats against which private sector facilities must be able to defend with high assurance. The DBT elements and characteristics form the design basis for physical security, defensive strategies, and guard force size and capabilities. The NRC rigorously inspects and tests the ability of these facilities to meet the DBT through inspection, force on force exercises and other means. This ensures that these facilities are demonstrably prepared to defend themselves. Any additional protective measures to defend against threats beyond the DBT are the responsibility of the Federal government in coordination with State and local governments, as well as owner/operators working together in a cooperative and collaborative manner.

The nuclear industry, NRC, and DHS recognize this delineation of private and public responsibility. DHS reviews all threats including those that affect nuclear power plants and is responsible for establishing appropriate responses to those threats. Through the performance of Comprehensive Reviews at commercial nuclear power plants and other critical infrastructure, DHS is identifying additional measures that will enhance the protection of critical infrastructure against a broad spectrum of threats.

[Another paragraph will go here discussing the relationship between the NRC and DHS in regard to the DBT]

For more than 25 years, NRC regulations have required rigorous security programs at certain nuclear facilities. Licensees have implemented these programs such that nuclear facilities are among the best-defended and most hardened commercial facilities in the Nation. Following the attacks on September 11, 2001, NRC required security enhancements. The security

enhancements include measures to provide additional protection against vehicle bombs, as well as water and land-based assaults. The NRC also required nuclear facility licensees to assess the potential impact of a terrorist-initiated event on site emergency plans. Additionally, the NRC's emergency preparedness experts routinely observe security exercises to assess and improve the interface between security plans and emergency plans. The NRC has substantially increased coordination with Federal, State, and local agencies.

A protective program is a coordinated plan of action to prevent, deter, and mitigate terrorist attacks on critical assets, and to respond to and recover from such acts as quickly and effectively as possible. With cooperation from the public and private sector partners, DHS serves as the national focal point for the development, implementation, and coordination of protective programs, including cybersecurity efforts, for those assets that are considered critical on the national scale.

Nuclear power plants in the United States are owned and operated by a variety of entities. For decades, these facilities have been licensed and regulated by the NRC. The NRC has the responsibility for protecting public health and safety, the environment, and the common defense and security from the effects of radiation from commercial nuclear reactors, materials, and waste facilities. To accomplish this goal, the NRC established a regulatory program containing requirements that must be implemented by licensees at nuclear power plants to protect the spent fuel and the power plant against radiological sabotage.

Commercial nuclear power plants have security measures in place to defend against a broad spectrum of potential terrorist threats, which are designed to prevent the release of radioactive material into the environment. The many layers of protection offered by robust plant design features, sophisticated surveillance equipment, physical security protective features, professional security forces, and access authorization requirements provide an effective deterrent against potential problems related to terrorist activities that could target equipment vital to nuclear safety. Were a terrorist attack to inflict damage on a nuclear plant, the redundant design features and the high level of training would likely result in actions taken by the plant staff to prevent or minimize the release of radioactive material. The emergency response plans would also provide for protective actions for the surrounding population were a release to occur.

The NRC has a continuing inspection program to review the security program at each nuclear plant to ensure safety, security, and continued compliance with NRC regulations. The NRC also has a regulatory program containing requirements for the physical protection of licensed materials at fuel cycle facilities and stored spent fuel at independent spent fuel storage installations (ISFSIs). Transportation of spent nuclear fuel and other high-activity shipments is protected using a variety of security measures.

As part of the national effort to protect critical infrastructure assets, DHS/RMD assists State and local authorities, and private industry, in developing BZPPs. The purpose of a BZPP, and protective measures planning in general, is to develop effective preventive measures that make it more difficult for terrorists to conduct surveillance or launch attacks from the immediate vicinity of CI/KR targets. In the case of a nuclear power plant, the BZPP concept defines a buffer zone outside of the facility's owner-controlled area. DHS contributes to the security measures in this sector through the application of the BZPP to augment security provided by plant operators. This plan engages local law enforcement agencies (LLEAs) to provide an additional layer of planned protection for facilities in this sector.

DRAFT

5.1 Overview of Sector Protective Programs

The implementation of protective programs in the Nuclear Sector is how risk is actually reduced. All the steps leading up to this, including identifying assets, systems, networks, and functions, assessing risk, and prioritizing help to identify where protective programs should be implemented, but what reduces the risk is the implementation of the protective programs themselves. After protective programs have been implemented, there will be the opportunity to measure the effectiveness of the programs and make adjustments as necessary.

The Nuclear Sector's protective programs address the full spectrum of protective activity, which includes: awareness, prevention, protection, response, and recovery. The goals of the Nuclear Sector also cover this entire spectrum. Because there is the obvious preference, though, to avoid a terrorist incident from happening in the first place, rather than respond and recover after one has occurred, more emphasis is placed on activities to deter and defeat terrorist attacks, through awareness, prevention, and protection. However, preparedness in the area of response and recovery is also very important.

Similarly, the outcome of the sector's protective programs range from deterring, detecting, devaluing, and defending against an attack to responding, mitigating, recovering from an attack, with somewhat more of a focus on the former than the latter due to the desire to stop an successful attack from happening in the first place.

The amount of progress made on the Nuclear Sector's goals and objectives, measured via the Nuclear Sector's metrics, will give a good indication on whether adjustments need to be made in the sector's overall security strategy. Also, the amount of risk associated with the Nuclear Sector will provide valuable input on how the sector is progressing.

The protective programs in the sector are discussed in more detail in the rest of this chapter and Appendix 2: Protective Programs. The NRC's regulations and recommendations can be considered one very large protective program, while DHS has a number of other protective programs.

CNPPD, as well as the rest of the GCC, recognizes the importance of non-Federal stakeholders, including the private sector and other levels of government, furthering efforts to protect the sector through developing protective programs of their own. CNPPD and the rest of the GCC will work to further strengthen the partnership among all of these stakeholders to assist such non-Federally developed protective programs in succeeding and addressing the most critical needs.

Protecting cyber elements of the Nuclear Sector is a critical part of the overall protection of the sector, and Goal #5 addresses the need to prevent cyber assets from being exploited. This includes the sector implementing NRC recommended cyber security programs at all the commercial nuclear power plants and ensure that the industry maintains awareness of the latest cyber security measures developed or recommended by DHS/NCSD, US-CERT, and other government-industry bodies concerned with cyber security. This includes the secure US-CERT portal, and its successor, the HSIN-Cyber portal. The Nuclear Sector will also continue to consider participating in other federal cyber programs and exercises. Government and the private sector need to work together in order to accomplish this, and the partnership between the two has already been displayed through both working together in creating and approving

DRAFT

NEI 04-04, as described in section 3.1.3. Following this strategy will help the Nuclear Sector prevent, protect, respond to, and recover from a cyber attack.

5.2 Determining Protective Program Needs

DHS/CNPPD will work with the other stakeholders within the Nuclear Sector, including the private sector and the GCC, to determine needs, based upon risk, as well as the best course of action to reduce potential consequences and vulnerabilities. CNPPD, as the SSA, will maintain a list of the sector's needs. This list of needs will be validated by CNPPD, working with the rest of the sector's stakeholders, and detailed information about the specific characteristics of each need will be captured and recorded. The decision to address or not address specific needs will be based upon the impact on reducing risk and the cost-effectiveness of the necessary measures to address the need. Particular protective programs that meet a legitimate need will be implemented based on their particular characteristics, as well as the needs of the sector.

The process to decide whether a need should be addressed to minimize a gap involves determining the threshold for taking action, determining whether closing the gap is possible, and prioritizing the gaps to determine the order in which they are addressed. The amount of risk associated with a gap determines if that gap meets the threshold level. Determining whether closing the gap is possible often involves a feasibility study. Prioritizing what gaps are addressed involves the amount of risk that can be reduced, and the cost-effectiveness of the risk reduction measure. There also needs to be a decision made if the cost of implementation of the protective measure is worth the cost of reducing the risk associated with the gap, and consideration needs to be given if any existing protective programs can also be used to address the gap at less cost. In addition, CNPPD will work with the NRC and other stakeholders in order to consider any existing regulations or standards that might aid or inhibit the implementation of a protective program.

The process to develop a new program in the absence of an existing program involves a number of steps, including identifying the need, developing potential solutions to meet the need, determining which solution would work best, pilot the test solution, evaluate the pilot, make refinements, and implement the protective measure on a large scale. The success of any protective program, whether new or existing, is based in large part to the participation of relevant stakeholders giving their input and providing their cooperation. Initiatives of owners and operators have been and continue to be welcome contributions in protecting the sector.

The NRC defines prevention, protection, response and recovery requirements for Nuclear Sector licensed facilities. These requirements are detailed, robust and measured regularly through inspection and drills. More discussion about the NRC role in regulating these is available in the NRC Information Digest. Details of these security requirements as well as specific security plans, strategies, and measures utilized to defend at commercial nuclear power plants and Category I fuel cycle facilities are filed with the NRC, but are not available to the public.

5.2.1 Decision-Making Processes

5.2.1.1 Roles and Responsibilities of Sector Stakeholders

Licensees are required to protect public health and safety by applying security measures at nuclear power plants and other facilities, and by complying with the regulations and other

DRAFT

requirements established by the NRC. In particular, the requirements established separately for each category of licensed activity or licensee specifies security measures appropriate for that category of facility or activity. For example, power reactor licensees are required to protect against attacks by adversaries whose purpose is to defeat or destroy the protective systems, prevent the safe operation of the licensed entity, and create a situation that would endanger the public by exposure to radiation. State and local governments, and, in certain situations, Federal agencies, may be called upon to augment security provided by licensees in protecting the facilities or activity, or responding to threats of theft or radiological sabotage.

In addition to ensuring safety and security, licensees operating large nuclear facilities are responsible for onsite emergency response to radiological emergency events. They are required to maintain an adequately trained staff to provide initial facility accident response, available timely augmentation of response capabilities, an adequate emergency plan, and facilitates to support interfaces among various onsite and offsite support and response activities.

The NRC coordinates incident response actions under the National Response Plan (NRP) and associated annexes including the Nuclear/Radiological Response Incident Annex for incidents involving NRC-licensed facilities and activities. In coordination with DHS, the NRC is also initiating integrated response planning to factor tabletop exercises (focusing on crisis and consequence planning, and emergency response exercises) into its planning basis, in accordance with the national preparedness goal. In the spring of 2005, the NRC updated its incident response program documents and procedures in order to comply with the NRP implementation deadline. The updates included the deletion of references to superseded national-level documents, re-defining NRC incident response modes to better comply with the current threat environment, and incorporating several terminology and organizational changes defined within the NRP.

When the NRC considers regulations and changes to the DBT, the cost to comply to the changes is not a factor in the NRC's decision making process, because the changes are of such criticality that their implementation can not be in doubt. However, in other cases, a balance must be struck between balancing costs of protective measures versus the risks for particular assets. DHS is involved with several initiatives, including BZPPs, Comprehensive Reviews or CRs (which are explained in more detail in section 5.3.1.3), and RAMCAP (detailed in chapters 3 and 4), which help the Nuclear Sector find ways to improve protective measures at a reasonable cost. Also, Industry's Security Working Group (SWG) assesses cost-benefits of protective measures on a regular basis.

The DHS/SSA works with State and local law enforcement and the NRC to develop BZPPs in the vicinity of commercial nuclear power plants and other assets within this sector. Selection of particular assets is commensurate with their risks. Working to address risk-based priorities, DHS provides funding to States for enhanced protective measures in the buffer zones surrounding nuclear facilities in this sector. Conducting BZPPs for commercial nuclear facilities is a very important part of Goal #4, which involves coordination with LLE.

DHS/FEMA's radiological emergency preparedness program responsibilities encompass offsite activities. These State and local government emergency preparedness activities take place beyond the nuclear facility boundaries. State and local governments are responsible for offsite emergency response to radiological emergency events within the EPZs. Emergency plans and preparedness provide reasonable assurance that appropriate protective measures can be taken offsite in the event of a radiological emergency.

DRAFT

Regulating the safety of radioactive material shipments is the joint responsibility of the NRC and the DOT. Both agencies establish requirements for the design and manufacture of packages for radioactive materials. The DOT regulates the shipments while they are in transit and sets standards for labeling. While safety regulation is the responsibility of NRC and DOT, security regulation is the responsibility of the NRC, DHS, DOT, and DOE. Following September 11, 2001, NRC, DOT, DOE, DHS/TSA and DHS/USCG have worked together to expand necessary security enhancements for radioactive material transportation.

5.2.1.2 How Critical Information Generated from Plan Implementation, Particularly the Information on Which Assets Appear to Pose the Highest Risk, Will Be Considered

The NRC regulates the nuclear industry and oversees implementation of its protective systems. In that role, the NRC also reviews, approves, and, if necessary, orders programs and systems designed to protect the plant from an attack by adversaries.

The NRC developed a new threat advisory and protective measures system that corresponds to the color-coded HSAS that allows Government officials to consistently communicate the nature and degree of terrorist threats nationwide. The NRC's system identifies specific actions to be considered by various classes of NRC licensees for each threat level to counter projected terrorist threats. If a credible threat emerges against a specific nuclear facility, additional protective measures may be implemented, even without a change in the overall threat level. As noted above, the NRC has issued regulatory issue summaries to help guide its licensees in implementing the HSAS.

The critical information generated in this review of risk posed by assets is considered sensitive and treated accordingly. Depending on the type of licensee, the information may be sensitive unclassified safeguards information in accordance with Section 147 of the Atomic Energy Act, or may be classified as national security information (NSI). This information is shared with the DHS/SSA through the NRC Operations Center and the DHS/SSA's HSOC. The NRC shares information and priorities, threats, and security measures with DHS, FBI, the intelligence community, and other Federal and State agencies and licensees.

5.3 Protective Program Implementation

5.3.1 Use of best practices and information sharing in encouraging stakeholder implementation

The nuclear power industry is a well-integrated industry of major corporations that have benefited from a collegial approach to design, maintenance, operation, and protection of assets in the Nuclear Sector for decades. From this experience, licensees have developed continuing means of communicating and sharing information, both within NRC-sponsored programs and among themselves. The NRC works with Nuclear Energy Institute (NEI) to address power reactor licensee concerns in an integrated fashion. The NRC routinely works with the NEI and licensee representatives to share best practices and security measures. For example, NRC and NEI meet at least monthly to discuss current issues related to nuclear power plant security. The NRC also shares DHS and FBI bulletins, advisories, and threat messages with licensees and other stakeholders through a secure protected Web server. NEI representatives, with Electric Power Research Institute (EPRI) contractors, cleared at the Secret NSI level, have participated in numerous meetings with the NRC staff concerning SAs. These industry representatives have participated in technical meetings concerning the NRC's SAs with the ACRS, and have also

DRAFT

attended NRC's Commission briefings. Some results of industry-sponsored assessments have been discussed with NRC staff, and the NRC has described its analysis method and results with cleared industry representatives. The NRC also participates in security working groups to better focus on the real-world concerns of its stakeholders.

Additionally, the DHS Comprehensive Review (CR) program identifies best practices and security measures and shares them with the NRC and industry through direct reports. The CR program and the BZPP likewise identifies best practices and security measures among LLE and emergency medical and emergency response (EM/ER) organizations. Methodologies for tracking implementation of potential enhancements and more formally sharing lessons learned and best practices are being considered.

5.3.2 How often and by which entity the protective programs will be updated and refined

Changes to the acceptable level of required programs, such as security or emergency preparedness, the policies and requirements in these arenas, and the protective strategies reflected in the licensees' security plans, have been, and will continue to be, included as part of the regulatory process of review and approval by the NRC. Protective programs initiated by the DHS/SSA will be updated and refined as coordinated through the DHS/SSA.

General approaches for protecting assets include:

Prevent or delay an incident—Nuclear facilities vary in the degree to which they are required to provide fixed security measures, based on the risk that the facility or activity presents to the public. The measures are required by the NRC in its regulations, license conditions, and orders. Security programs for nuclear power plants and certain fuel cycle facilities include protective layers (e.g., owner controlled area, protected area, and vital area/materials access area), physical barriers (e.g., personnel, vehicle, and water), intrusion detection devices, alarm stations, redundant communications systems, armed security organizations with response guards specifically trained and detailed to those functions, comprehensive background checks for personnel with access to protected areas, fitness-for-duty programs for the workforce, and procedures to integrate State and local resources into their response to malevolent attacks on the facility.

Detect a potential incident—Licensees at high-risk facilities have programmatic elements that are part of a mandated security program.

Mitigate or respond to an incident—Licensees at high-risk facilities have contingency plans approved by the NRC that include integration of site security forces with resources provided by State and local government agencies. These plans require the facility to maintain an armed security organization, with response officers specifically trained and detailed to protect the assets in this sector.

Recovery from an incident—Licensees' safeguards contingency plans include steps to recover control of the facility and resume operation and/or render the facility safe. The licensees have plans in place for the coordination of these efforts with Federal, State, and local law enforcement agencies. DHS, in partnership with the NRC, DOJ, DOD, and other Federal agencies, has undertaken pilot integrated-response exercises at two power reactor facilities, and further initiatives to strengthen integrated response at power reactor and Category I fuel cycle facilities are under consideration.

DRAFT

5.3.2.1 Commercial Nuclear Reactors, Fuel Cycle Facilities, Spent Fuel Storage Facilities, and High-Level Waste Disposal Facilities

Nuclear facilities that require physical protection include nuclear reactors, Category I fuel cycle facilities, spent fuel storage facilities, and high-level waste disposal facilities. Key features of the physical protection programs for these facilities include:

- Defense in depth, using graded physical protection areas: exclusion area, controlled access area, protected area, vital area, and material access area barriers and controls
  - The exclusion area is that area in which the licensee has the authority to determine all activities including exclusion or removal of personnel and property.
  - A controlled access area is any temporarily or permanently established area with clear demarcation, access to which is controlled, and which affords isolation of the material or persons within it.
  - The protected area is an area within the exclusion area encompassed by physical barriers, such as one or more chain-link fences.
  - Vital areas are located within protected areas, and have additional barriers and alarms to protect vital equipment.
  - Material access areas are any locations containing special nuclear material, within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.
- Intrusion detection
- Assessment of detection alarms to distinguish between false or nuisance alarms and actual intrusions and to initiate response
- Response to intrusions
- Offsite assistance, as necessary, from local, State, and Federal agencies

In August 2002, the NRC implemented a threat advisory and protective measures system based on the HSAS to communicate and respond to threats affecting sector-regulated facilities and activities. The system provides a consistent national framework for allowing the NRC to communicate the nature and degree of terrorist threats to licensees. When DHS raises the national threat level, the NRC promptly advises licensees operating nuclear power reactors and other sensitive nuclear facilities about the increase in the threat level and the need to implement pre-planned protective measures commensurate with the threat level. The protective measures associated with the HSAS procedures and other security enhancements required by the NRC generally include specific actions against attacks by land, water, and air.

In addition, the NRC has an on-going program to assess the availability of additional mitigative measures to enhance the safety of licensed commercial nuclear power plants. This effort is proceeding in three phases, the first of which was to identify readily available measures that could be brought to bear in a short time frame. The second and third phases of this mitigative strategy effort will look for additional, readily available measures and 'beyond readily available" measures to address the safety of the spent fuel pool (Phase 2) and the reactor core and containment structures (Phase 3). The NRC began site-specific spent fuel pool assessments (Phase 2) on July 5, 2005 in order to identify additional enhancements to safety of the spent fuel pool cooling features under severe circumstances. The Phase 2 assessments were completed

DRAFT

in November 2005. Plant-specific Phase 3 assessments were begun in September 2005 and are scheduled for completion in April 2006.

In addition, following the terrorist attacks of September 11, 2001, the NRC evaluated the EP planning basis, issued orders requiring compensatory measures for nuclear security and safety, and observed licensee performance during security-based EP drill and exercises and security force-on-force exercise evaluations. The NRC staff also discussed security-based EP issues with various stakeholders, including licensees and Federal, State, and local government officials. Based on the information obtained, the NRC staff determined that the EP planning basis remains valid, but recognized that security events differ from accident-initiated events. In July 2005, the NRC issued NRC Bulletin 2005-02,"Emergency Preparedness and Response Actions for Security-Based Events" to commercial nuclear power reactor licensees. This bulletin provided guidance on enhancements to emergency preparedness programs for response to a security-based event. Also, based on NRC guidance, certain types of nuclear facilities will develop pilot EP-security based integrated response exercise program consisting of two tabletop exercises and one drill to be completed within one year. In addition, every nuclear power reactor facility will have completed a security-based scenario in the form of an NRC-observed drill, or an NRC/FEMA-evaluated exercise within four years.

5.3.2.2 Transportation

The transportation of nuclear and radioactive materials requires certain protective measures. There are four broad categories of this material (strategic special nuclear material (SSNM), spent nuclear fuel (SNF), RAMQC, and HRCQ). The following key features of the transportation protective measures apply to these materials, in whole or in part, depending on the security risk:

- Use of NRC-certified shipment transportation packages designed to withstand certain hypothetical accidents. The robustness of some packages also provides a degree of security (e.g. spent fuel package)
- Advance notifications to NRC and affected States, planning, and coordination with local law enforcement along transportation routes
- Protection of shipment information as classified or sensitive unclassified as appropriate.
- Regular communication between transports and control centers
- Escorts (armed for some shipments)
- Vehicle immobility measures to protect against movement of a hijacked shipment before response forces arrive

Associated with the improving tracking for legitimate shipments of radioactive materials objective of Goal #3, there are currently several international and federal-level efforts being directed at security of radioactive material in transport. The international strategy for controlling radioactive sources includes the establishment of global safety and security standards and import/export controls. Led by the U.S., the International Atomic Energy Agency (IAEA) developed and adopted two instruments to secure and control radioactive sources: the Code of Conduct on the Safety and Security of Radioactive Sources (Code) and the Guidance on Import and Export of Radioactive Sources (Guidance). The leaders of 77 IAEA members have currently agreed to implement the Code and work toward following the Guidance. The IAEA is also developing additional security related companion guidance for transport of radioactive

DRAFT

material, to supplement the safety requirements. Security related guidance is also being developed to support radioactive material transit and transshipment evolutions that do not have an origination or final destination point within a given country. To support this effort, the NRC is sponsoring a Transit Transshipment Security Working Group (TTSWG) to formulate a proposal for the Department of State to take forward to the IAEA for either a revision to the Code of Conduct or to be used as supplemental guidance. Additionally, DHS has initiated a tri-lateral Security and Prosperity Partnership for security of radioactive material that includes Canada and Mexico. Finally, as described in section 3.7, the Energy Policy Act of 2005 requires the NRC to promulgate regulations establishing a mandatory tracking system for radiation sources in the U.S. and establishes a task force on Radiation Source Protection and Security to evaluate and provide recommendations to Congress and the President on the security of radiation sources in the U.S.

5.3.2.3 Radioactive Material Users and Sources (risk-significant radioactive material)

The users of the radioactive materials in quantities of concern and special nuclear material apply safeguards to protect against sabotage, theft, and diversion, including:

- Physical protection of facilities, radioactive materials in quantities of concern, and/or special nuclear material both at fixed sites and during transportation
- MC&A for radioactive materials in quantities of concern and special nuclear material

The NRC has issued orders for enhanced security and safeguards measures to certain materials licensees who possess radioactive materials in quantities of concern and special nuclear material. The requirements of these orders have since been codified in NRC regulations. MC&A is associated with the control of a facility's personnel access to, use of, and transfer of nuclear materials; and monitoring the status of materials to prevent losses, or detect losses should they occur. It consists of access control, containment, surveillance, item monitoring, and bulk material monitoring measures. Material accounting maintains knowledge of the locations and quantities of nuclear materials, and provides for physical inventories and material balances to verify the presence of materials, or to detect losses after they occur. It includes measures such as data records and measurements.

Since September 11, 2001, the NRC has been thoroughly re-evaluating its safeguards and security programs to determine actions needed in order to enhance the safety and security of radioactive materials licensed by the NRC for medical, industrial, and academic uses. The emphasis of this re-evaluation has been on preventing the use of materials that present higher risks to public health and safety if deployed in an RDD. The objectives of the NRC's programs to control radioactive materials are to ensure the protection of the public and the environment, and to promote the Nation's common defense and security. The overall approach is risk-informed, focuses on radioactive materials of greatest concern, and uses measures based on a computational methodology that systematically evaluates radioactive materials for RDD concerns. The actions taken and the goals for continuing efforts to enhance security are to ensure that:

- RDD attacks are prevented by identifying, adequately securing, and appropriately monitoring radioactive materials of greatest concern (prevent events)
- Response organizations are adequately prepared for a potential RDD attack (limit consequences of events)

DRAFT

- International and domestic organizations are addressing RDD issues in an integrated, consistent manner (communication and coordination)

In addition to measures intended to prevent the malevolent use of radioactive materials in quantities of concern, other materials used in a wide range of applications beyond the scope of nuclear power, fuel cycle, nonpower reactors and waste facilities require certain protective measures commensurate with the form and quantity of material as well as the radionuclide.

The NRC has taken additional steps to heighten the security posture, including new measures taken to protect certain regulated transportation activities. These measures were implemented through the issuance of orders for shipments of spent nuclear fuel and for RAMQC. Advisories were issued to specify which shipments require notification to NRC. The current physical protection measures for risk-significant radioactive material transportation include:

- Preshipment coordination with law enforcement agencies
- Preshipment notice of States and NRC
- In-transit shipment call-in to communications center
- Shipment monitoring
- Escorts, if necessary

Both the NRC and DOE continue joint operation of a national database and information support system to track movement of special nuclear materials under safeguards control. The National Source Tracking System is expected to be made available to all authorized Federal departments and agencies once completed.

In developing protective programs for radioactive material users, this sector generally uses working groups composed of representatives from the NRC, Agreement States, and other Federal agencies, as appropriate, to formulate a proposed strategy for individual initiatives; the NRC then approves each proposed action. Actions are implemented either by rule making, order, or license amendment. Each implementing process includes stakeholder interactions to review and comment on the proposed actions. Stakeholder interaction is consistent with the sensitivity of the proposed action. In some cases, such as work-hour controls for security-force personnel, broad public interaction is undertaken. In most circumstances, the sensitivity of the protective action requires involvement only of cleared stakeholders. Based on stakeholder input, the proposed actions are revised and submitted to the NRC for final approval. For recent security orders issued by the NRC, regional meetings were conducted with the specific categories of licensees and Agreement State regulators to discuss proposed actions, and to obtain comments on the proposed action and implementing guidance. Where practicable, industry representative groups may propose industry-specific implementing guidance that could be adopted by the NRC. Ultimately, any enhanced protective measures implemented by order or license amendment will be codified into the NRC's regulations.

5.3.2.4 Personnel at Nuclear Power Plants and Category I Fuel Cycle Facilities

Besides threats from outsiders, insider threats must also be considered in protecting assets within the sector. Therefore, various employees require licensing and background investigations in order to work in nuclear power plants or Category I Fuel Cycle Facilities.

DRAFT

Licensed Nuclear Power Plant Operators. The NRC licenses the individuals operating the controls of nuclear power plants. There are two categories of licenses: reactor operator and senior reactor operator. A senior reactor operator is a supervisory position overseeing the work of the reactor operators. The license is issued after the individual passes both a written examination and an operating test. The senior reactor operator examination also measures the ability of the individual to direct the activities of other licensed operators.

Moreover, all licensed operators and senior operators are required to participate in their facility licensee's drug and alcohol testing programs, and are prohibited from using, possessing, or selling illegal drugs, and from performing licensed duties while under the influence of alcohol or any prescription, over-the-counter, or illegal substance that could adversely affect their performance.

Security Personnel at Nuclear Power Plants. Owner/operators of commercial nuclear power plants are required to establish and maintain a security force that, in the face of a malevolent act detailed in the design basis threat (DBT) against the facility, would ensure that plant operators and safety systems retain the capability to safely shut down the reactor, assure long-term decay heat removal, and prevent radiological sabotage. The NRC made changes to enhance security requirements in a February 25, 2002, order, and revised the DBT in an April 29, 2003 order. The DBT describes the attributes of the threat against which owner/operators must defend their facilities. These security personnel are trained in threat identification, weapons handling, and tactical response, including frequent firing of weapons, realistic training under different conditions, and firing against moving and fixed targets. Owner/operators of commercial nuclear power plants made substantial improvements to security force training, and established work-hour controls for security force personnel, based upon two other April 29, 2003 NRC orders.

The security force at every commercial nuclear power plant demonstrates their ability to defend the plant against the DBT through a force-on-force exercise every three years. The security force is challenged by a trained adversary force with significant facility information and advanced tactics. This is a graded exercise overseen by the NRC.

Security Personnel at Category I Fuel Cycle Facilities. Similar to the requirement imposed upon nuclear power plant licensees, Category I fuel cycle facility licensees are required to maintain a security force that can prevent the theft or diversion of SSNM when faced with a threat characterized by the DBT. The NRC made changes to enhance security at Category I fuel cycle facilities in an August 2002 order, and revised the DBT in an April 29, 2003 order.

Other Nuclear Facility Personnel. All nuclear power plants, along with facilities licensed to possess, use, or transport formula quantities of SSNM, have fitness-for-duty programs to provide reasonable assurance that plant personnel will perform their tasks in a reliable manner; that they are not under the influence of any substance, legal or illegal, which may impair their ability to perform; and that they are not mentally or physically impaired from any cause which can adversely affect their ability to competently perform their duties.

In the 1980s, the NRC began to focus on the integral role that humans play in the safe operation of a nuclear power plant and certain fuel cycle facilities. The NRC published the Fitness-for-Duty (FFD) Program (10 CFR Part 26) rule in 1989; which requires licensees to implement an FFD program for all personnel with unescorted access to nuclear power plant protected areas, or those personnel who are granted unescorted access to SSNM at a Category I fuel cycle facility that is directly usable in the manufacture of nuclear weapons.

DRAFT

Employee Background Investigations. In addition to the above precautions, the NRC requires expanded, expedited, and more thorough background check conducted by the licensee, for nuclear power plant employees to ensure that they are reliable and trustworthy. Every employee with access to safety equipment is required to pass a background check, including an examination of past employment, references, credit history, educational history, military history, military service history, and an FBI criminal history records check. Employees also undergo psychological testing and a continual behavior observation program. The NRC substantially improved its access authorization program in a January 2003 order. Employees of Category I fuel cycle facilities are required to have a security clearance based on a background investigation conducted by the federal government.

5.3.2.5 Provide Protective Security Support to Communities

1. The Department of Homeland Security will provide protective security support to communities via the use of its network of Protective Security Advisors (PSAs). Members of the protective community charged with safeguarding Nuclear Sector will benefit from this support. To better partner with State governments, local communities, and the private sector, DHS placed a cadre of experienced security specialists, PSAs, in neighborhoods throughout the country to assist local efforts to protect critical assets and also provide a local perspective to the national risk picture. PSAs are DHS employees with an average of 20 years of anti-terrorism and security experience and function as liaisons between DHS, the private sector, and Federal, State, Territorial, local, and tribal entities. PSAs are recruited from, live, and work in local communities and thus have an in-depth knowledge of critical infrastructure and key resources (CI/KR) in their assigned area of responsibility, or district. PSAs maintain strong working relationships with local stakeholders, to include law enforcement and owners and operators CI/KR. They act as DHS' on-site critical infrastructure and vulnerability assessment specialist; provide expertise and support to the Principal Federal Official(s) responsible for domestic incident management and special events planning; and provide real-time information on facility significance and protective measures. PSAs will also assist with ongoing local and state critical infrastructure security efforts which are coordinated by the state Homeland Security Advisors; facilitate the flow of programmatic information between stakeholders; assist in the coordination of training and exercises; serve as advisors regarding local infrastructure during activation of the National Response Plan; and provide reach-back capability to DHS and other Federal government resources.

5.3.3 Comprehensive Reviews

5.3.3.1 Purpose and Scope of Comprehensive Reviews

A Comprehensive Review (CR) is a cooperative government and private sector analysis of CI/KR facilities that considers potential terrorist actions for an attack, the consequence of such an attack, and the integrated prevention and response capabilities of the owner/operator, local law enforcement, and emergency response organizations. The results are used to enhance the overall security posture of the facilities using short-term and long-term risk based investments in training, processes, procedures, equipment, and resources for the community.

For the first time, Federal agencies are meeting together with industry representatives, owner/operators, local law enforcement, and emergency responders to conduct a joint analysis

DRAFT

of the multiple functions required to detect, deter, defend, mitigate, and respond to potential terrorist attacks.

CRs are being conducted of all commercial nuclear power reactors and associated (spent fuel storage) facilities.

The NRC strictly regulates all facets of operating the nation's commercial nuclear power reactors. Unlike previous security assessments of these sites, the Comprehensive Review will also include an examination of the areas outside the perimeter of the facilities, including surrounding water elements, and community emergency response capabilities.

CRs are an important aspect of accomplishing Goal #7, using a risk-informed approach for security decisions, and Goal #9, using a risk-informed process for potential emergency response enhancements.

5.3.3.2 Nuclear Sector Lead in Comprehensive Reviews

While Comprehensive Reviews will be performed in other sectors, the Nuclear Sector is the first to participate in this process. Factors contributing to the readiness of the Nuclear Sector and its selection as the first in which CRs have been conducted include the support of the private sector, the high level of a stable baseline of security, and the early recognition by DHS and the NRC of the importance of cooperating in a post-September 11, 2001 environment. As of December 2005, 14 CRs have been completed.

As each sector has unique characteristics, some aspects of CRs may vary in other sectors, as the CRs will be tailored to the given sector. In the future, conducting CRs on other subsectors within the Nuclear Sector will be considered. CRs for other nuclear subsectors could also vary to some degree.

5.3.3.3 Coordinating Federal, State, Local, and Private Sector Efforts

In its role as Federal coordinator, DHS will lead CR teams composed of experts from the NRC, FBI, USCG, and FEMA. Because the nation's commercial nuclear power infrastructure is almost totally owned and operated by the private sector, DHS recognizes the importance of a continued government/industry partnership. Therefore, DHS has established the Nuclear Sector Government Coordinating Council (GCC) and the Nuclear Sector Coordinating Council (NSCC), the private sector equivalent of the GCC, to coordinate enhanced security of the nation's nuclear power assets.

5.3.3.4 Nuclear Sector Comprehensive Review Process

Each team will meet for an orientation prior to the actual site visit. A logistics team will provide evaluation tools and site reference material to each review team. This time will be used to study the site and focus on identifying the consequence and critical asset information provided by the owner/operator, and the various existing security and emergency plans to ensure the CR team is familiar with site-specific characteristics and capabilities.

Following the orientation, the review team will deploy for a three-to-five day site visit. During the site visit, the team will work with site personnel, especially engineering, safety, security, and emergency planning staff as well as senior management. The review team also meets with

DRAFT

critical community response agencies including local, county, and State law enforcement and emergency management leadership to evaluate community-wide readiness and preparedness capabilities.

5.3.3.5 Comprehensive Review Results

The information that derived from this joint and collaborative review process will be used at a number of levels to ensure the long-term security of the nation's critical infrastructure assets.

The results will be documented in a formal report for the appropriate stakeholders, including the various Federal agencies involved, facility owner(s)/operator(s), local, county and State law enforcement, and emergency response services. The report will include the following:

- An Executive Summary
- A site-specific Integrated Protective Measures Plan (IPMP) that will identify resource gaps, coordination issues, assessment of response capabilities, training needs, and options for potential enhancements to address protective and response challenges. The IPMP will coordinate response plans, ensuring that responders and equipment are adequate to meet planned roles and operate in concert under differing scenarios.

The data collected during the site visits across the country will also serve to develop an overall picture of the readiness of the entire sector and will further assist in identifying industry best practices in security and response measures.

In addition, the information gathered during the CR process will be used in reviewing other critical infrastructure assets in a different sector that are in close proximity to the sites that are reviewed. Comprehensive Review results will further yield normalized risk data across critical infrastructure sectors that will inform DHS investment decisions in the future.

5.3.3.6 Benefits of the Nuclear Sector Comprehensive Reviews

The benefits include:

- Facilitating the comparative risk assessment of commercial nuclear power reactors using a standardized methodology that produces a measurable baseline, thereby allowing the future assessment of the efficacy of protective response measures and planning.
- Improving coordination among industry, owners/operators, local law enforcement, emergency responders, and governments to prevent, mitigate, and respond to a potential terrorist event.
- Establishing joint efforts among all stakeholders to reach decisions on best practices in protective and response measures that will be most appropriate for a given site or across the sector.
- Supporting DHS and other Federal agency investment and budgeting decisions, allowing for the most efficient and coordinated allocation of resources across multiple sectors.

DRAFT

5.3.4 NRC Rulemaking

5.3.4.1 Design Basis Threat Rulemaking

The DBT requirements in 10 CFR 73.1(a) describe general adversary characteristics that designated licensees must defend against with high assurance. The NRC requirements include protection against radiological sabotage (generally applied to power reactors and Category I fuel cycle facilities) and theft or diversion of NRC-licensed SSNM (generally applied to Category I fuel cycle facilities). The DBTs are used by these licensees to form the basis for site-specific defensive strategies implemented through security plans, safeguards contingency plans, and guard training and qualification plans.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place for the changing threat environment. In so doing, the NRC recognized that some elements of the DBTs required enhancement due to the escalation of the domestic threat level. After soliciting and receiving comments from Federal, State, local agencies as well as industry stakeholders, the NRC imposed by order supplemental DBT requirements which contained additional detailed adversary characteristics. The balance between licensee responsibilities and the responsibilities of the local, State and Federal Governments was considered during the development of the April 29, 2003, DBT orders. The NRC's decision was based on the analysis of intelligence information regarding the trends and capabilities of the potential adversaries and discussions with Federal, law enforcement, and intelligence community agencies. The NRC's DBT is not based on worst-case scenarios but rather on actual adversary characteristics demonstrated worldwide and a determination as to those characteristics against which a private security force could reasonably be expected to provide protection.

The NRC is currently conducting a rulemaking as a follow-up to the April 29, 2003, orders. The revised rule will incorporate the attributes of the orders as well as a re-evaluation of the threat. The proposed rule and supporting documentation will be published in the Federal Register for public comment.

5.3.4.2 Security Requirements Rulemaking

Along with the changes to the DBT, the NRC specified changes to requirements for specific training enhancements and enhancements to defensive strategies as provided in site security plans and site contingency plans. Additionally, through generic communications, the NRC's Commission expressed expectations regarding enhanced notification to the NRC regarding security events.

By October 30, 2004, all of the nuclear power plant licensees had revised and approved training plans, security plans, and contingency plans in place. These plans incorporated the enhancements instituted through the April 2003 orders. While the specifics of these changes are sensitive, in general they resulted in enhancements such as increased patrols, augmented security forces and capabilities, additional security posts, additional physical barriers, vehicle checks at greater standoff distances, enhanced coordination with law enforcement and military authorities, augmented security and emergency response training, equipment, and communication, and more restrictive site access controls for personnel, including expanded, expedited, and more thorough employee background checks.

DRAFT

The NRC is currently conducting a rulemaking which will consolidate the supplemental requirements put in place by the orders and the existing requirements in 10 CFR 73. The proposed rule language will describe the security requirements at a level of detail appropriate for public discussion. Specific details related to the requirements that are safeguards information (SGI) will be consolidated in regulatory guidance documents that will be available only to those with appropriate clearance and need to know.

5.4 Protective Program Performance

Chapter 6, Measure Progress, details a number of metrics associated with the Nuclear Sector's goals and objectives. The impact that a given protective program has on meeting one or some of these goals, objectives, and metrics is one way to determine the program's effectiveness. Even if the protective program is not specifically included in this document's goals, objectives and metrics for the sector, each protective program should still have its own metrics used to measure its effect. These metrics will be reported on an annual basis.

CNPPD, as the SSA, along with the NRC, the rest of the GCC and the private sector, is involved in recommending improvements to the sector's processes and mechanisms for communicating successes and recommendations. CNPPD, again working with the other stakeholders, has the lead for ensuring that future decision-making will utilize information gained from protective program performance monitoring.

Following R&D relevant to the Nuclear Sector, which will be discussed further in Chapter 7, is very important in the process to monitor technological developments that might improve or modify protective programs. Technology improvements can sometimes be applied across multiple protective programs, where the technology is first applied to one program, then the performance benefits are tested, and then the technology is applied to other protective programs as well.

5.5 Challenges

5.5.1 Integrated Response

There are numerous Federal, State, and local agencies and organizations with emergency response or preparedness responsibilities. Integration challenges and competing prioritizations between these various emergency organizations are important to resolve. DHS and the NRC are working with these agencies and organizations, along with owners and operators of other key resources and critical infrastructure, to ensure adequate preparation for and response to a terrorist attack at a nuclear facility.

5.5.2 Reactor Licensees

Physical protection programs at commercial nuclear power plants have come under extensive scrutiny in the aftermath of September 11, 2001. While security plans were robust prior to the terrorist attacks on our country, the NRC and the industry are now implementing measures to further enhance plant security, and are considering additional measures.

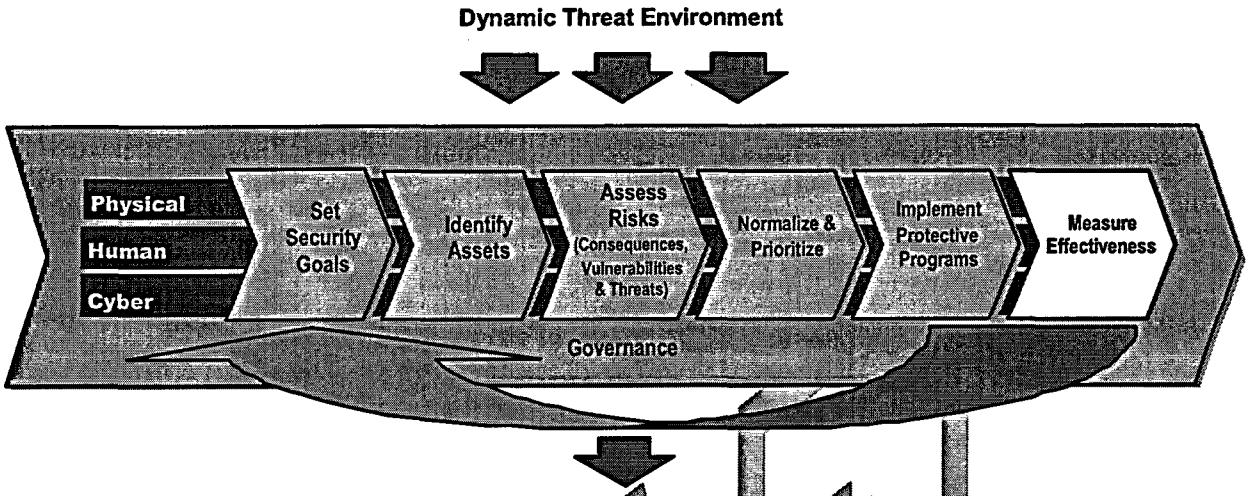
DRAFT

5.5.3 Control of Radioactive Materials in Quantities of Concern

There are thousands of facilities in the United States licensed to possess and/or use sources containing risk-significant isotopes. These radioactive materials in quantities of concern and their uses have been accurately characterized in previous sections of this document. Proper accountability and control of these sources can only be ensured by the NRC and Agreement States through aggressive and well-thought-out regulation. The NRC is working with Federal, State, and private industry stakeholders to ensure that the users of radioactive materials in quantities of concern are complying with the proper usage and accountability regulations. Protection of these sources is important in order to prevent RDD and RED proliferation.

DRAFT

6 Measure Progress



Critical infrastructure protection (CIP) metrics have been broken into two categories: core metrics and sector-specific metrics. The core metrics will be tracked across each sector to enable comparison and analysis between and among different types of critical infrastructure. DHS/SSA and security partners will work together to establish a data-gathering and reporting process. Specific issues such as responsibilities, procedures for the gathering and reporting of information, as well as timelines will be worked out in this process.

The sector-specific metrics are outcomes descriptive of the issues related to protection of the assets in this area. These metrics are connected with the Sector Security Goals, detailed in Chapter 3. The determination on how successful the sector is in meeting the goals set for it will be measured using the sector-specific metrics described below.

6.1 CI/KR Performance Measurement

There are two types of CIP metrics: core and sector-specific. Core CIP metrics, common across all sectors, are a set of primarily process measures that will measure initial progress in sector-specific plan implementation. These metrics fit into the overarching framework of Nuclear Sector measures, and are aligned with the key steps in the CIP program implementation process. Sector-specific metrics are specifically associated with the goals and objectives for the Nuclear Sector.

Both types should be considered initial metrics, with each evolving as DHS and the nuclear stakeholders become more knowledgeable on their specific CIP challenges. These metrics will serve to meet DHS' needs to monitor performance across all sectors.

DRAFT

6.1.1 Developing Sector-Specific Metrics

6.1.1.1 Utilize Core CIP Metrics Defined by DHS

Core metrics, which are common across sectors, are still being developed by DHS. However, a list of sample core metrics include:

1. Total number of assets by class
2. Number of assets with potential for medium or high consequences
3. Percentage of medium- and high-consequence assets with completed vulnerability analyses
4. Percentage of medium- and high-consequence assets rated at high risk
5. Percentage of medium- and high-consequence assets that have active protective programs to measurably reduce risk
6. Percentage of medium- and high-consequence assets that have been assessed for readiness, response, and recovery capability
7. Percentage of formal security-partner agreements by sector and geographic location
8. Percentage of assets reduced from high risk

Information on the core CIP metrics will be maintained in a database of nuclear assets by the SSA; the database will be developed in coordination with NRC. DHS/SSA will provide guidance on the necessary periodicity or metric reports as part of the plan enhancement, prior to the 1-year update.

6.1.1.2 Sector Security Goals and Metrics

Most of the sector-specific metrics are tied to one of the objectives associated with an individual sector security goal. Therefore, the following set of metrics are shown in the context of which sector security goal and objective with which the metric is associated.

6.1.1.2.1 ***Initial Process to Develop Metrics***

The metrics for the goals were initially drafted by the Nuclear SSP Working Group, which has representation from a wide spectrum of private and public sector entities. This Working Group met a number of times to develop and then revise the goals, objectives and metrics. The GCC and NSCC will review and approve the goals, objectives and metrics, prior to the publication of the final version of this Nuclear SSP.

6.1.1.2.2 ***Awareness Goal Metrics***

Goal #1: Establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities. (Office of Primary Responsibility (OPR): NRC, DHS)

DRAFT

- ❑ **Objective #1.1** – Define, identify and maintain the key points of contacts (POCs) having security and emergency response responsibilities for the Nuclear Sector. (OPR: NRC, DHS)
  - Metric #1.1.1 – Update a comprehensive list of stakeholders having security and emergency response capabilities and responsibilities that is reviewed by the NSCC, GCC, and States on an annual basis. (OPR: NRC, DHS)
- ❑ **Objective #1.2** – Communicate clear, timely, and comprehensive threat and intelligence information as appropriate. (OPR: CNPPD)
  - Metric #1.2.1 – Time needed to get threat and intelligence information from DHS to the private sector. (OPR: CNPPD; Office with Supporting Responsibility (OSR): HITRAC)
  - Metric #1.2.2 – Percentage of industry representatives that are cleared to receive classified threat and intelligence information, out of the set of industry representatives that should be cleared to receive such information. (OPR: NRC, DHS)
  - Metric #1.2.3 – Percentage of organizations with cleared representatives that receive classified threat briefings. (OPR: NRC, DHS)
- ❑ **Objective #1.3** – Increase public awareness of the consequences and proper actions following a release of radioactive material. (OPR: DHS; OSR: NSCC, NRC, DOE)
  - Metric #1.3.1 – Percentage of people surveyed who indicate they have an understanding of what to do if a radioactive release occurs. (OPR: DHS)
- ❑ **Objective #1.4** – Increase public awareness of protective measures in place in the Nuclear Sector, at a level of detail that would help deter, rather than encourage or help enable, a terrorist attack. (OPR: DHS; OSR: NSCC, NRC, DOE)
  - Metric #1.4.1 – Percentage of people surveyed who believe that a successful terrorist attack associated with the Nuclear Sector would be difficult to accomplish. (OPR: DHS)
- ❑ **Objective #1.5** – Share lessons-learned from previous nuclear and radiological events within the sector (OPR: CNPPD)
  - Metric #1.5.1 – Percentage of nuclear subsectors for which there has been an evaluation to determine if a program exists for the sharing of lessons-learned. (OPR: CNPPD)
  - Metric #1.5.2 – Percentage of nuclear subsectors that have a lessons-learned sharing program for which the federal government is one source for lessons-learned. (OPR: CNPPD)

Goal #2: Determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector. (OPR: RMD)

- ❑ **Objective #2.1** – Identify Nuclear Sector dependencies and interdependencies in order to fully understand and plan for the consequences of an interruption of service from another critical infrastructure or key resource as well as consequences to other sectors. (OPR: RMD)

DRAFT

- Metric #2.1.1 – Percentage of commercial nuclear facilities that have developed a list of dependencies and interdependencies of other CI/KR, and developed contingency plans to deal with their loss. (OPR: CNPPD)

6.1.1.2.3 Prevention Goal Metrics

Goal #3: Prevent nuclear and radioactive material from being used for malevolent purposes. (OPR: DOE, DOD, DHS, DOJ)

- ❑ **Objective #3.1** – Improve capability to detect unauthorized nuclear and other radioactive materials at key U.S. entry points where these materials either enter the U.S. or pass through before being transported to other countries. (OPR: DHS, DOE, DOJ)
  - Metric #3.1.1 – Number of key U.S. entry and pass through locations with the capability to detect nuclear and radioactive material. (OPR: DHS)
- ❑ **Objective #3.2** – Improve capability to detect unauthorized shipments of nuclear and other radioactive materials within the U.S. (OPR: DHS, DNDO/OSE, DOE, DOT)
  - Metric #3.2.1 – Number of key transportation hubs within the U.S. with the capability to detect nuclear and radioactive material. (OPR: DNDO/OSR, DHS, DOT)
- ❑ **Objective #3.3** – Improve security for legitimate shipments of nuclear and radioactive materials physically transported in the United States, using a graded approach.[28] (OPR: DOT)
  - Metric #3.3.1 – International transport security regulations proposal submitted to and adopted in International Atomic Energy Agency and United Nations transport regulations. (OPR: DOT; OSR: DHS, NRC, DOE, DOS)
  - Metric #3.3.2 – Written agreement reached among the involved agencies on the roles and responsibilities. (OPR: CNPPD; OSR: DOE, DOT, NRC, DOS)
  - Metric #3.3.3 – Percentage of SSNM, SNF, RAMQC, and HRCQ shipments with unregulated security requirements but voluntary compliance implemented when physically transported in the United States. (OPR: DHS; OSR: NRC, DOE, DOT)
- ❑ **Objective #3.4** – Improve security and tracking of all high-risk (Category 1 and 2) sources that are in legitimate use within the U.S. (OPR:TBD)
  - Metric #3.4.1 – Percentage of high-risk (Category 1 and 2) sources within the U.S. that are registered in the National Source Tracking System (OPR: TBD)
  - Metric #3.4.2 – Percentage of high-risk (Category 1 and 2) sources registered in the National Source Tracking System that are in commercial use and have had their security reviewed. The review will take place starting with those sources of greatest threat. (OPR: TBD)

[28] This objective includes developing a program of interaction among the Department of State (DOS), NRC, DOT, DOE, and DHS (CNPPD/RMD/Domestic Nuclear Detection Office [DNDO]/US Coast Guard [USCG]), which considers private sector input, to clearly define the roles and responsibilities associated with tracking legitimate shipments of nuclear and radioactive material into or through this country, with international support and consensus, by identifying gaps and recommending enhancements to close gaps.

DRAFT

- ❑ **Objective #3.5** – Through grant programs, improve capabilities of the private sector to better secure their risk-significant (Category 1 and 2) sources. (OPR: TBD) [placeholder objective]
  - Metric #3.5.1 – Percentage of high-risk (Category 1 and 2) sources within the U.S. that have increased security meeting national requirements. (OPR: TBD) [placeholder metric]
- ❑ **Objective #3.6** – Through grant programs, locate and recover risk-significant (Category 1 and 2) sources that are declared excess and unwanted. [placeholder objective]
  - Metric #3.6.1 – Amount of risk-significant (Category 1 and 2) sources that are recovered. (OPR: TBD) [placeholder metric]

Goal #4: Coordinate with Federal, State, and local Law Enforcement Agencies to develop tactics to deter, detect and prevent terrorist attacks on fixed nuclear facilities. (OPR: RMD)

- ❑ **Objective #4.1** – Develop Buffer Zone Protection Plans (BZPPs) for all commercial nuclear power reactors (and associated spent fuel facilities) and fuel cycle facilities by December 2007. (OPR: RMD)
  - Metric #4.1.1 – Percentage of fixed commercial nuclear power reactors (and associated spent fuel facilities) and fuel cycle facilities that have BZPPs in place. (OPR: RMD)
- ❑ **Objective #4.2** – Work with local authorities to develop plans to identify and secure radioactive sites. (OPR: TBD)
  - Metric #4.2.1 – Percentage of Urban Area Security Initiative (UASI) local authorities assisted. (OPR: TBD)
- ❑ **Objective #4.3** – Increase local authorities' awareness of consequences of malicious use of risk-significant (Category 1 and 2) sources. (OPR: TBD) [placeholder objective]
  - Metric #4.3.1 – Number of local authorities made aware of need to have adequate source security measures. (OPR: TBD) [placeholder metric]

6.1.1.2.4 Protection, Recovery, and Response Goal Metrics

Goal #5: Protect the cyber assets of the nuclear sector from being exploited. (OPR: CNPPD, NRC, private sector)

- ❑ **Objective #5.1** – Implement the NRC recommended cyber security programs at all the commercial nuclear power plants. (OPR: private sector)
  - Metric #5.1.1 – Percentage of the commercial nuclear power plants that have implemented the NRC recommended cyber security programs. (OPR: NRC)
- ❑ **Objective #5.2** – Ensure that the industry maintains awareness of the latest cyber security measures developed or recommended by DHS/National Cyber Security Division (NCSD) and by other government-industry bodies concerned with cyber security. (OPR: CNPPD)

DRAFT

- Metric #5.2.1 – Percentage of nuclear cyber security industry personnel who have subscribed to the secure US-CERT portal and its successor, the HSIN-Cyber portal. (OPR: CNPPD with IPD support, private sector)

Goal #6: Utilize R&D to better protect the Nuclear Sector from future threats. (OPR: DHS)

- ❑ **Objective #6.1** – Create an annual report summarizing the R&D planning process results. (OPR: CNPPD)
  - Metric #6.1.1 – Whether or not the annual list of R&D priorities has been sent to DHS S&T and OSTP. (OPR: CNPPD)
  - Metric #6.1.2 – Whether or not an annual list of gaps has been created and prioritized, based upon a review of the Nuclear Sector technology requirements and the current R&D initiatives product review. (OPR: CNPPD)
  - Metric #6.1.3 – Whether or not an annual report summarizing the R&D planning process results is created utilizing the list of gaps. (OPR: CNPPD)

Goal #7: Use a risk-informed approach that includes security considerations to make budgeting, funding, and grant decisions on all identified potential protection and emergency response enhancements. (OPR: CNPPD)

- ❑ **Objective #7.1** – Complete CRs of existing commercial nuclear power reactors by December 2007. (OPR: CNPPD; OSR: RMD, NRC, private sector)
  - Metric #7.1.1 – Percentage of commercial nuclear power reactors that have had CRs performed on them. (OPR: CNPPD)
  - Metric #7.1.2 – Percentage of potential enhancements identified during the CR process that have been implemented. (OPR: CNPPD)
  - Metric #7.1.3 – Percentage of potential enhancements identified during the CR process, which require grant assistance for implementation, for which there has been a grant application submitted. (OPR: CNPPD)
- ❑ **Objective #7.2** – Complete assistance visits to selected Research and Test Reactors (RTRs) by the end of December 2006. (OPR: CNPPD; OSR: RMD, NRC, private sector)
  - Metric #7.2.1 – Percentage of selected RTRs that have had an assistance visit to their facility. (OPR: CNPPD; OSR: RMD, NRC, private sector)
- ❑ **Objective #7.3** – Evaluate other subsectors within the sector to determine which warrant assessments, prioritize the order of assessments, and complete assessments in the chosen areas by December 2010. (OPR: CNPPD; OSR: RMD, NRC, private sector)
  - Metric #7.3.1 – Percentage of the subsectors evaluated to determine which subsectors warrant assessments. (OPR: CNPPD; OSR: RMD, NRC, private sector)
  - Metric #7.3.2 – For those sector elements that the determination was made to perform assessments, the percentage of facilities that have had assessments performed on them. (OPR: CNPPD; OSR: RMD, NRC, private sector)
- ❑ **Objective #7.4** – Ensure that each facility in a nuclear subsector, which is above a certain risk-threshold, has an emergency response plan commensurate with the level of risk associated with the facility. (OPR: CNPPD; OSR: RMD, NRC, private sector)

DRAFT

- Metric #7.4.1 – For those subsectors that the determination was made to verify emergency response plans, the percentage of facilities that have had their emergency response plan verified to ensure it includes the appropriate material.(OPR: NEI)

Goal #8: Enhance the ability of the Federal, State, Territorial, tribal, local, and private sector to effectively respond to nuclear and radiological emergencies as a result of terrorist attacks, natural disasters, or other incidents. (OPR: CNPPD)

- ❑ **Objective #8.1** – Review and revise, as appropriate, the Nuclear/Radiological Incident Annex to the National Response Plan to better delineate the roles and responsibilities of Federal departments and agencies in preventing, preparing for, responding to and recovering from nuclear or radiological incidents. (OPR: FRPPC)
  - Metric #8.1.1 – Revise the Nuclear/Radiological Incident Annex by December 2006. (OPR: FRPPC)
- ❑ **Objective #8.2** – Incorporate emergency preparedness (EP)-security-based scenarios into the Emergency Preparedness drill and exercise programs for commercial nuclear power facilities. (OPR: DHS, NRC)
  - Metric #8.2.1 – Each nuclear power reactor facility will integrate security events fully into the drill and exercise program to the extent that one biennial exercise per six-year period is an EP-security exercise. (OPR: NEI)
  - Metric #8.2.2 – Percent of other commercial nuclear facilities within the Nuclear Sector that annually or more frequently conduct security drills responding to simulated terrorist attacks. (OPR: NEI)
- ❑ **Objective #8.3** – Incorporate prompt notification technologies such as Automated Ring Down circuits between the DHS NICC and all Cat 1 and NPP's within the sector. (OPR: DHS, NRC)
  - Metric #8.3.1 – Percent of Cat 1 and NPP's within the Nuclear Sector with installed Automated Ring Down telecommunications capability with the DHS NICC. (OPR: DHS)
  - Metric #8.3.2 – Percent of cross-sector CI/KR near Cat 1 and NPP's with Automated Ring Down telecommunications with the DHS NICC. (OPR: DHS)

6.1.2 Information Collection and Verification

The Office of Primary Responsibility (OPR) and Office of Supporting Responsibility (OSR) have been determined for each goal, objective, and metric. They will provide a vital role as the agency responsible for determining the means of assessing the metric, as well as collecting and verifying sector-specific metric information and submitting that information to the SSA. Additionally, the SSA may call on the various agencies for assistance in collecting and verifying information on the core metrics.

The OPR and OSR will have the responsibility for determining the validity of the information that is submitted. One method for verifying accuracy is through the submission of official documentation that supports the information being collected. Metrics will be assessed and information collected and reported on an annual basis, unless stated otherwise. Some of the information that is collected may be sensitive or proprietary and protocol for protecting this

DRAFT

information will be followed. Section 2.5 contains information on how sensitive or proprietary information is handled and protected.

6.1.3 Reporting

The SSA has responsibility for collecting data on the metrics from the OPR, and OSR if applicable, of each metric. The format used to assess the metric will be determined by the OPR. On at least an annual basis, the SSA will report to the GCC and the NSCC on the progress in accomplishing the goals as well as any gaps that may be found in existing goals. Also, HSPD-7 calls for sectors to report annually to the Secretary of Homeland Security on progress. In many instances, it may be useful for sector security partners to know the status of a metric. The SSA may determine whether a metric should be shared with stakeholders and can utilize any of the information sharing mechanisms to do so.

6.2 Implementation Actions

The following table contains implementation actions described throughout this document.

[Material will be added to this table shortly. The table will not contain new material, but just reflect what has been discussed in the rest of the document]

Action	Responsible Stakeholders
Letter of Agreement and Support	
Introduction	
Chapter 1: Sector Profile and Goals	
Chapter 2: Identify Assets, Systems, Networks, and Functions	

DRAFT

Chapter 3: Assess Risks	
Chapter 4: Prioritize Infrastructure	
Chapter 5: Develop and Implement Protective Programs	
Chapter 6: Measure Progress	
Chapter 7: CI/KR Protection R&D	
Chapter 8: Managing and Coordinating SSA Responsibilities	

DRAFT

6.3 Challenges and Continuous Improvement

It is important to incorporate metrics into the decision-making process. In an effort to do so, the SSA, in coordination with the GCC and NSCC, will reexamine the metrics, along with the goals and objectives, on an annual basis, or more frequently if necessary, considering changes in the sector's security posture, to determine if any modifications should be made. In providing quantitative and qualitative feedback, metrics are necessary tools for indicating whether or not progress is being made towards achieving sector goals. If the SSA, GCC, or NSCC determine

that there is not sufficient progress being made towards a particular goal, the SSA can work with the OPR and OSR, if applicable, to address the concern.

Though this set of metrics is believed to be robust, having incorporated efforts to ensure the metrics are both measurable and comprehensive, there will still be room for improvement. Updating and refining the metrics will take place during the annual SSP revision process. Also, changes in the sector's security posture will result in changes to the objectives and metrics.

Identifying and implementing measures to improve the Nuclear Sector's security posture involves reassessing risk in a changing security environment, and by taking action on those items that address areas of greatest risk or are cost-effective solutions that, in combination, reduce risk the most. This approach will be used in modifications to the goals, objectives, and metrics.

DRAFT

7 CI/KR Protection R&D

7.1 Overview of Sector R&D

Through technological advances, Research and Development (R&D) programs can provide cost-effective and efficient means of utilizing limited resources. Effective R&D programs will result in mitigating risk in the sector at low enough costs that regardless of budget capabilities, all security partners can enjoy the benefits.

As the SSA for the Nuclear Sector, DHS/CNPPD communicates R&D needs to support the DHS/Science and Technology Directorate (S&T) and Office of Science and Technology Policy (OSTP) in cooperation with the NRC, DOE, DHS/DNDO and DOT as supporting agencies. There will be formal efforts to communicate these R&D needs on an annual basis, and other less formal communication on an as needed basis. Also, DHS/S&T has the primary responsibility to develop the annual National Critical Infrastructure Protection R&D Plan, and CNPPD, as the SSA, will provide input into that. DHS/S&T is represented on the GCC, and this helps to enable the dialogue between CNPPD and DHS/S&T.

Each supporting agency maintains its own R&D planning process, and CNPPD, as the SSA, integrate sector needs. CNPPD will collect input on the sector's R&D needs on an ongoing basis from all sector stakeholders. Some of the potential benefits of R&D that CNPPD will consider, when evaluating the Nuclear Sector's R&D needs, are: 1) ensuring the compatibility of communications systems with interoperability standards; 2) exploring methods to authenticate and verify personal identity; 3) coordinating the development of Nuclear Sector protection consensus standards; and 4) improving technical surveillance, monitoring, and detection capabilities.

Cyber R&D needs will be considered along with non-cyber R&D needs. The group of stakeholders with which CNPPD coordinates cyber R&D needs will be slightly different than other R&D needs, and includes DHS/NSCD among others. CNPPD will solicit information from NCSD, DHS/S&T, and OSTP about ongoing R&D initiatives that may help the sector meet cyber security-related technology requirements.

As expressed in Goal #6 and corresponding objectives and metrics, technology development is necessary and therefore one of the top priorities in the Nuclear Sector is to better utilize R&D which will help protect the sector from future threats.

7.2 Sector R&D Requirements

To support development of the Federal CIP R&D plan, DHS/SSA will communicate sector R&D requirements to DHS S&T and OSTP. The DHS/SSA will request and integrate inputs from the NRC, DOE, and DOT as supporting agencies as well as other sector stakeholders on an ongoing basis. Supporting agencies will coordinate with appropriate stakeholders in developing inputs. Prior to engaging supporting agencies, DHS/SSA will solicit information relative to the themes that DHS S&T and OSTP have identified for integration across sections. Supporting agencies will identify requirements relative to these themes. The SSA will work with security partners to collect and prioritize capability requirements that can be supported by technology developments. This information can then be used to determine whether current R&D programs meet the requirements or whether new programs may be needed.

DRAFT

7.3 Sector R&D Plan

7.3.1 Current R&D Initiatives

In conjunction with the determination of the technology requirements above, the SSA will annually provide supporting agencies with a listing of the current Federal R&D initiatives. The source of this list is DHS/S&T and OSTP. The SSA will coordinate a review of sector challenges, technology requirements, and current Federal R&D initiatives with the sector-supporting agencies and DHS/S&T and OSTP. Sector-supporting agencies will coordinate with and represent the views of their sector stakeholders. The product of this review will include a prioritization of the current Federal initiatives relative to the sector challenges and performance measures. Some of the factors that will be considered during this review are: need; the potential impact in reducing risk that could result from the R&D; cost-effectiveness; likelihood of success of the R&D effort; and amount of time estimated that will be needed from the start of the R&D effort to implementing the technology in protective measures. The SSA will provide the product to the DHS/S&T and OSTP.

7.3.1.1 DOE Activities

DOE is leading a multinational effort in the development of a fourth generation nuclear power plant. The goals of that effort are enhanced proliferation resistance, improved economy of operation, and enhanced environmental friendliness. The Secretary of Energy, and four other nations including Japan, France, Canada, and the United Kingdom, signed a framework agreement to proceed on the fourth generation nuclear plant development on February 28, 2005.

DOE is leading a multi-agency effort to develop classification guidance for transportation of spent nuclear fuel and high-level radioactive waste to the Yucca Mountain repository. At DOE's invitation, the NRC, the DOT, and the DHS are taking joint action to harmonize their guidance in this area.

DOE is leading a multiphase, multinational spent nuclear fuel sabotage program. Participants include the NRC and international partners from Great Britain, Germany and France. The International Working Group for Sabotage of Transport and Storage Casks has identified three projects:

- The first project involves the experimental determination of the radioactive source term released to the environment as a result of transportation sabotage and the environmental consequences of this radioactive release.
- The second project involves development a risk-based approach for comparing a wide range of terrorist attacks on various transportation targets.
- The third project, which is pending, will involve the development of sabotage barriers for transportation and storage casks.

DOE is developing a Multilateral Agreement that would permit the exchange of classified information on these projects.

DRAFT

7.3.1.2 DHS DNDO Activities

The DNDO is currently developing the next generation of passive radiation portal monitors through the Advanced Spectroscopic Portal (ASP) program. ASP systems address a substantial capability gap in currently deployed systems by increasing the probability of detecting a smuggled nuclear device, while decreasing the probability of falsely alarming on naturally occurring radioactive materials or innocent radioactive materials (such as granite tiles, ceramics, and kitty litter) or incorrectly dismissing nuclear material. ASP systems use their ability to identify the source of detected radiation through spectroscopic isotopic identification to accomplish this.

The DNDO is developing the next generation of active imaging radiography systems through the Cargo Advanced Automated Radiography Systems (CAARS) program to automate radiographic image processing, as well as provide considerable improvements in the rate of radiographic inspection. It will scan cargo containers or other conveyances of interest and provide an automated alert based upon the threat. The implemented technology will distinguish between low density non-threat materials such as aluminum and steel, and higher density materials such as lead, uranium or plutonium. CAARS will also be capable of the detection of traditional contraband such as high explosives and drugs, but may not do so with the same level of automation. Search for traditional contraband will continue to require operator image analysis.

The DNDO systems development program also includes a program to deliver to the U.S. Government, advise State/Territorial/local government awareness of next generation handheld and man-portable systems required by operators such as the U.S. Coast Guard, CBP, Border Patrol, State, Territorial, local and tribal law enforcement agencies and first responders. These handheld, mobile and backpack systems are used as primary detection tools by our Border Patrol and USCG personnel subsequent to interdiction. CBP uses this equipment as a secondary inspection tool, while State, Territorial, local and tribal law enforcement agencies and first responders may use this equipment for queued search and secondary identification.

In FY 2006, the DNDO will begin the initiatives that will develop regional deployment strategies aimed at achieving the most effective and integrated use of detection equipment for domestic detection and interdiction. The initiatives will provide design engineering support to State and local agencies in the development of procurement, deployment and lifecycle upgrade strategies suited to their individual locale. This support will enable the DNDO to ensure that State and local agencies will acquire and deploy systems with proven performance characteristics, that these deployments are consistent with the global detection architecture, and that they will be interoperable with the DNDO Joint Analysis Center (JAC). State and local agencies must purchase equipment, as well as related training, exercise, and support packages, using Federal grant funding, thus freeing up the Federally-owned equipment for use in additional engagements.

7.3.1.3 NRC Activities

The NRC process for planning and budgeting its research activities is consistent with the strategies and measures in the NRC's FY 2004-2009 Strategic Plan. As key uncertainties in analyses that influence the agency's ability to make realistically conservative decisions are identified, safety-focused research is proposed to address uncertainties that are amenable to being reduced through research. These candidate research programs are prioritized according to their contribution to accomplishing strategic goals. For example, one of the NRC's strategic

DRAFT

goals is to enable the use and management of radioactive materials and nuclear fuels for beneficial civilian purposes in a manner that 1) protects public health and safety, and the environment, 2) promotes the security of our Nation, and 3) provides for regulatory actions that are effective, efficient, realistic, timely, and open. A research activity is considered "high" if it is a significant contributor to the strategies to be used to accomplish a goal (e.g., if accomplishing the activity is critical to being able to implement the strategies to accomplish a goal). It is "medium" if it directly contributes (e.g., if accomplishing the activity supports being able to implement the strategies to accomplish a goal), and "low" if it has a less-substantial contribution. The expected outcomes of NRC activities associated with this strategic goal include: (1) no nuclear reactor accidents; (2) no releases of radioactive materials that result in significant radiation exposures; (3) no acute radiation exposures resulting in fatalities; and (4) no releases of radioactive materials that cause significant adverse environmental impacts.

Research activities are prioritized along with other NRC activities, and a research budget is established. Activities with relatively low-ranking scores are dropped or delayed if the NRC's budget cannot support those research activities. The NRC will coordinate through DHS/SSA to communicate identified R&D needs to DHS S&T and OSTP annually.

NRC coordinates inter-agency R&D planning and activities through the Counter-Terrorism Technical Support Office, Technical Support Working Group and DOD's Physical Security Advisory Group.

7.3.2 Gaps

DHS/SSA will request a review by DHS S&T and the DHS DNDO Joint Requirements Board (JRB), or OSTP of the sector technology requirements and current R&D initiatives product. The product of the review is to be an identification of the gaps between sector technology requirements and current R&D initiatives. Department of Homeland Security/SSA will review these gaps with the sector-supporting agencies to prioritize the significance of the gaps, and summarize the most important gaps for the sector.

7.3.3 Planned R&D Initiatives

The gap prioritization analysis performed by DHS/SSA and the sector-supporting agencies will be forwarded to DHS S&T, OSTP, and DHS/JRB with a request for identification and description of R&D initiatives that potentially fill identified gaps. DHS/SSA will review the initiatives provided with sector supporting agencies to determine relevancy to the sector. The output of this review is to be a report back to DHS S&T, OSTP and DHS/JRB summarizing the R&D planning process results, including: technology requirements, current R&D initiatives, gaps, candidate R&D initiatives, relevance of R&D initiatives to the sector, and gaps that are not addressed by the candidate R&D initiatives.

7.4 R&D Management Processes

CNPPD, as the SSA, will continue to monitor the progress of R&D development, assess its impact on the sector goals, and update its R&D strategy as needed. In order to accomplish this, CNPPD will work with the GCC, SCC, and other stakeholders. CNPPD will also keep apprised of non-Nuclear Sector specific R&D efforts that could have benefits to the Nuclear Sector, through information provided by DHS/S&T, OSTP and others.

DRAFT

The transition process from R&D to implementing the technology in protection programs in the field is also critical to the success of R&D efforts. Each R&D technology will require at least a slightly different implementation path, due to each technology's unique characteristics. However, in most cases, there will be a pilot project where the technology is implemented out in the field prior to its widespread use. CNPPD will work with the appropriate stakeholders to identify the best implementation process for a given technology.

DRAFT

8 Managing and Coordinating SSA Responsibilities

8.1 Program Management Approach

Within CNPPD, there is a program management office in place in order to fulfill CNPPD's Nuclear SSA responsibilities listed throughout this document. The staff of the program management office tracks the responsibilities of CNPPD in order to ensure the completion of those tasks. In many cases, CNPPD will coordinate with the other stakeholders in the sector to verify that their responsibilities listed in this document have also been fulfilled.

In the Nuclear Sector, there is already a large amount of cooperation and coordination that takes place among sector stakeholders, including interaction between the private sector and government. CNPPD's philosophy is to take the strong relationships that exist today, and continue to grow those, and when appropriate, foster new relationships.

The chart in section 6.2, listing implementation actions associated with this document, will be used as a starting point in ensuring that key processes will be implemented and monitored.

CNPPD will evaluate the structure of its program management office periodically, to ensure that the structure is the most effective one to meet its responsibilities.

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

The Nuclear SSP is one of the primary planning and management documents associated with the Nuclear Sector. As the Nuclear Sector's security status will continue to change, revisions to the document will be considered on at least an annual basis, with a full rewrite of the document every three years. The Nuclear SSP Working Group, which provided a coordination mechanism to allow input from both industry and government into the document, will be the primary body responsible for making those changes. The GCC and the NSCC will approve the modifications to the Nuclear SSP.

CNPPD will work with the rest of DHS, other federal agencies, State and local governments, the private sector and other security partners to aggregate information and build a comprehensive picture of Nuclear Sector infrastructure protection efforts across the nation. This will assist DHS in understanding how CI/KR protection is being conducted across the country, what priorities and requirements drive these efforts, and how such efforts are funded.

8.2.2 Annual Reporting

On July 1st of each year, the SSA will submit an annual CI/KR protection report on the Nuclear Sector to the Secretary of Homeland Security. Nuclear Sector protection requirements, NIPP-related initiatives, and relevant requirements for Nuclear Sector protection will be identified. The report will also include:

- Priorities and annual goals for Nuclear Sector protection
- Nuclear Sector requirements for CI/KR protection activities and programs based upon risk and need

DRAFT

- Projections for NIPP-related program funding that will be included in the SSA budget request to the Office of Management and Budget as part of the annual Federal budget process.

8.2.3 Resources and Budgets

CNPPD, as the SSA, will outline Nuclear Sector protection requirements and related budget projections as a component of the annual budget submission to the Office of Management and Budget (OMB). The process for determining which areas are considered priorities for the purpose of CI/KR protection funding will be based on cost-effectiveness and the reduction of risk.

In the February – July timeframe of each year, CNPPD will develop the NIPP-related aspect of their budget submission with the support of the rest of DHS where necessary and consistent with NIPP requirements established through the collaborative process. By September 1st of each year, CNPPD will work with the rest of DHS to rationalize individual requirements and recommend funding in the cases where gaps or duplicative efforts exist. Then, between September and November of each year, CNPPD will work the Office of Management and Budget (OMB) and the rest of DHS in subsequent budget deliberations to remedy any gaps or shortcomings in NIPP-related funding.

CNPPD will also serve as subject matter experts reviewing and providing recommendations for specific target grant programs, as well as working closely with the private sector to promote the most efficient use of both Federal and non-Federal resources.

8.2.4 Training and Education

Awareness is a critical component to the overall success of protecting the Nuclear Sector, and the first two Nuclear Sector goals focus on awareness. Goal #1 is to establish permanent and robust collaboration and communication among all stakeholders within the Nuclear Sector having security and emergency response responsibilities. Goal #2 is to determine the consequences of dependencies and interdependencies of other critical infrastructures and key resources to the Nuclear Sector. These efforts will go a long way to helping in to successfully protect the Nuclear Sector.

The Base NIPP states a number of objectives associated with a national awareness program, which DHS is working with the SSAs and other security partners to develop and implement. The Nuclear Sector will coordinate with the overall national awareness program to ensure that the efforts are in synch.

Periodic exercises and training involve not only the nuclear power plant plants themselves, but also the NRC, State and local governments and emergency response officials – including fire, medical, law enforcement and traffic control authorities. All these entities are also included in the licensee's emergency response plan.

Extensive training onsite and offsite is conducted periodically. Ongoing communication and regular drills and exercises ensure that the plant personnel and the community's emergency response organization are in the ready to protect the health and safety of the public.

DRAFT

Coordinated onsite offsite training often includes the following: Emergency Response Support; notification methods; emergency communications; public information, including dissemination of information and acquainting news media with emergency plans; accident assessment; protective response options; radiological exposure control, including decontamination procedures; specialized training and periodic retraining, including medical services and hospital support, fire and rescue, and local law enforcement.

DHS provides overarching coordination to the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition to the incident management framework established in the NRP. Some examples of national exercises are TOPOFF and Ardent Sentry. The SSA will coordinate sector-level participation in the National Exercise program and other sector-level preparedness activities. DHS/SSA will work to ensure that the National Exercise Program and National Cyber Exercises include adequate testing of steady-state CI/KR protection measures and plans, including information sharing; application of the risk management framework; and the ability to protect core of life-critical CI/KR services, such as power, food and water, and emergency transportation, to withstand attack or natural disasters and continue to function at an appropriate level.

The NRC provides some training to States, mainly to train inspectors of Agreement States. The NRC does not advocate or promote activity in the Nuclear Sector, in order to retain its neutrality as a regulator.

A combined effort of DHS/SSA, other federal agencies, and additional security partners will review and update existing CI/KR protection-related courses to align with the NIPP. Two areas within DHS that may offer such courses are DHS/Grants and Training and DHS/Risk Management Division (RMD). Additionally, in identifying and updating programs, CNPPD, Grants and Training, and RMD will work together to identify and fill any gaps that may exist.

Overall, the SSA will promote sector-level CI/KR protection education, training, and awareness.

8.3 Implementing the Sector Partnership Model

The Sector Partnership Model is the framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector owners and operators. Within most sectors, a Government Coordinating Council (GCC) exists to coordinate government efforts and a Sector Coordinating Council (SCC) exists to coordinate private sector efforts. The NIPP discusses the portion of the Sector Partnership Model that enables the all of the GCCs and SCCs to work together on issues applicable to more than one sector.

8.3.1 Coordinating Structures

The Nuclear Sector has both a Nuclear Sector Government Coordinating Council (GCC) and a Nuclear Sector Coordinating Council (NSCC). DHS/IPD will serve as a liaison between the NSCC and the GCC in its role to facilitate implementation of public-private partnerships. Both councils were established on October 13, 2004, and they held their first joint meeting on that day. The GCC and NSCC meet quarterly to continue developing this important partnership. The councils are part of the overall sector partnership model which is described in detail in the Base NIPP.

DRAFT

8.3.1.1 Nuclear Sector Government Coordinating Council

The objective of the GCC is to provide effective coordination of civilian nuclear security strategies and activities, policies, and communications across the government and between the government and the Nuclear Sector to support the nation's homeland security mission. In addition, the GCC plays a coordination role with the existing emergency management and public health and safety communities regarding response and recovery issues associated with a terrorist act involving the Nuclear Sector.

The GCC accomplishes this objective primarily through four types of activities. First, identify items that need public-private coordination, and the communication and coordination of those items. Second, identify needs/gaps in plans, programs, policies, procedures and strategies. Third, acknowledge and recognize successful programs and practices. And fourth, leverage complementary resources within government and between government and industry.

The GCC consists of representatives from:

- DHS/CNPPD
- DHS/RMD
- DHS/FEMA
- DHS/S&T
- DHS/USCG
- NRC
- FBI
- DOE

There may also be ad hoc or ex-officio members added to the GCC, and the DOD/Homeland Defense is a current ex-officio member. The DHS/CNPPD representative chairs the GCC and DHS/IPD provides secretarial support. Meetings are held quarterly, with additional meetings scheduled or conference calls held when needed.

8.3.1.2 Nuclear Sector Coordinating Council

The NSCC consists of representatives of the nuclear industry and covers the broad interests of Nuclear Sector security. The scope of the NSCC covers all companies licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major nuclear architect/engineering firms, fuel supply and fabrication facilities, research and test reactors, commercial nuclear waste management and transportation firms, and other organizations and individuals involved in the nuclear industry. There is also a Radioisotopes Subgroup of the NSCC for those in the industry that are involved in the use, manufacture, distribution, and disposal of radioactive materials beyond nuclear power and the fuel cycle.

DRAFT

Specific NSCC membership will consist of key representatives and senior decision makers involved in nuclear security issues at their respective companies. Makeup of the NSCC will generally conform to the following guidelines:

- Six members from companies owning or operating at least one commercial nuclear power reactor
- One member from owners of fuel manufacturing or fuel fabrication facilities
- One member from manufacturers of nuclear reactors or components
- One observer from the National Organization of Test, Research, and Training Reactors
- One member from a nuclear waste management or transportation company
- One member from NEI
- Representative(s) from the NSCC-Radioisotopes Subcouncil

The Nuclear Energy Institute (NEI) has a representative on the NSCC because NEI represents a large portion of the overall sector, including constituents of the Radioisotopes Subgroup. All domestic operators of commercial nuclear power plants and fuel processing facilities are members of NEI. Through NEI, the industry can undertake initiatives that commit the entire industry to specific actions.

The NSCC-Radioisotopes Subcouncil (NSCC-R) develops and recommends strategies that will enhance the physical security and emergency preparedness of the radioisotope sector under the auspices of the NIPP. NSCC-R voluntarily collaborates with the GCC to identify and recommend measures to prevent radioisotopes of concern from being stolen, diverted and used in Radiological Dispersion Devices (RDDs) or Radiological Exposure Devices (REDs). The outcome will be to ensure that the radioisotope sector continues to provide benefits for medical, industrial and research applications in a safe and secure manner while protecting the public health and safety.

The National Organization of Test, Research, and Training Reactors (TRTR) represents research reactor facilities across the nation from government, universities, national laboratories, and industry. TRTR's primary mission is education, fundamental and applied research, and application of technology in areas of national concern and improving U.S. technological competitiveness around the world.

8.3.1.3 Federal Radiological Policy Coordinating Committee

The Federal Radiological Policy Coordinating Committee (FRPCC) provides a national-level forum for the development and coordination of radiological prevention and preparedness policies and procedures. It also provides policy guidance for Federal radiological incident management activities in support of State, local, Territorial, and tribal government radiological emergency planning and preparedness activities. The FRPCC is an interagency body chaired by DHS/CNPPD. The FRPCC establishes subcommittees, as necessary.

The FRPCC also coordinates research-study efforts of its member agencies related to State, local, Territorial, and tribal government radiological emergency preparedness to ensure

DRAFT

minimum duplication and maximum benefits to State and local governments. The FRPCC coordinates planning and validating requirements of each agency, reviewing integration requirements and incorporating agency-specific plans, procedures, and equipment into the response system.

8.3.1.4 State, Local, Territorial and Tribal Government Entities

U.S. commercial nuclear power reactors have developed close relationships with local and State law enforcement agencies as well as emergency response organizations to achieve a high level of cooperation for emergency planning and response. This relationship will fully support the development of a sector-specific plan.

When considering State government entities, recognize that there are also thirty-three Agreement States which are listed in Table 2 in section 1.1.2.5. Agreement States are described in more detail in Section 1.2.1.5.

8.3.1.5 International

8.3.1.5.1 International Atomic Energy Agency (IAEA)

The IAEA, established in 1957, is an independent intergovernmental, science and technology-based organization, in the United Nations family, that serves as a global focal point for nuclear cooperation. The IAEA assists its 138 Member States, in the context of social and economic goals, in planning for and using nuclear science and technology for various peaceful purposes, including the generation of electricity, and facilitates the transfer of such technology and knowledge in a sustainable manner to developing Member States.

Part of the IAEA's mission involves developing nuclear safety standards and, based on these standards, promoting the achievement and maintenance of high levels of safety in applications of nuclear energy, as well as the protection of human health and the environment against ionizing radiation. The IAEA also verifies through its inspection system that Member States comply with their commitments, under the Non-Proliferation Treaty and other non-proliferation agreements, to use nuclear material and facilities only for peaceful purposes.

To assist Member States in the identification of the best means by which to strengthen their nuclear security, IAEA has initiated the International Nuclear Security Advisory Service (INSServ). Requested by a Member State, INSServ missions aim at identifying overall needs for additional or improved security measures for nuclear-related activities of the Member State, whether involving nuclear material and facilities or other radioactive material, such as radioactive sources, and relevant facilities. The INSServ mission generates recommendations, which provide the platform for subsequent, more specific, nuclear security assistance, either through IAEA programs or through bilateral support programs.

With the help of International Physical Protection Advisory Service (IPPAS) missions, the IAEA assists Member States in strengthening and enhancing the effectiveness of their physical protection of nuclear materials and facilities. An IPPAS mission may be conducted on a nation-wide basis, or it may be facility-specific. During the IPPAS mission, the Member State's physical protection system is reviewed and compared with the international guidelines and internationally recognized best practices. Based on this review, recommendations for improvements are provided including follow-up activities and assistance. Following the recommendations from

DRAFT

IPPAS missions, actual upgrades of physical protection systems have been initiated in several Member States, through bilateral support programs.

The IAEA also has missions to help smaller countries without nuclear programs to develop safety and security measures for sources and radioactive materials. An example is the Radiation Safety and Security of Radioactive Sources Infrastructure Appraisal (RaSSIA) mission.

8.3.1.5.2 Nuclear Energy Agency (NEA)

The NEA is part of the Organization for Economic Co-operation and Development (OECD). The NEA's mission is to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological, and legal bases required for the safe, environmentally friendly and economical use of nuclear energy for peaceful purposes. To achieve this, the NEA works as a forum for sharing information and experience and promoting international cooperation; a center of excellence which helps member countries to pool and maintain their technical expertise; and a vehicle for facilitating policy analyses and developing consensus based on its technical work.

NEA membership currently consists of 28 countries in North America, Europe, and the Asia-Pacific region. Together, the countries account for approximately 85% of the world's installed nuclear capacity. The NEA works closely with the IAEA.

8.3.1.6 International Nuclear Regulators Association (INRA)

Established in January 1997, the INRA's membership consists of the most senior officials of the nuclear regulatory authorities of the following countries: Canada, France, Germany, Japan, Spain, Sweden, the United Kingdom, and the United States. It provides a forum where the most senior regulators can identify nuclear regulatory challenges and exchange views on broad regulatory policy issues. Through its work, the INRA seeks to accomplish the following objectives:

- Build a global nuclear safety culture;
- Seek international consensus on approaches to nuclear safety issues and facilitate international cooperation to implement sound solutions;
- Cooperate with other international and national organizations involved in nuclear safety; and
- Encourage the most efficient use of resources.

8.4 Information Sharing and Protection

8.4.1 Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a highly secure network backbone built over the Internet with a common set of information sharing functions and tools for various communities consisting of people with a "common interest" (e.g., the Nuclear Sector). The Nuclear Sector is currently piloting usage of HSIN to support the Comprehensive Review (CR) Program and provide threat-warning products. HSIN's benefits include: information sharing and

DRAFT

coordination enhancements within each community; a built-in capability for cross-community-of-interest and public-private sector information sharing once "communities" are established; and a common platform for growth and improvements in the future.

Two of the many other parts of HSIN are:

- Critical Infrastructure Warning Information Network (CWIN) – A private government network within HSIN that provides mission-critical connectivity and a survivable DHS capability for information sharing, collaboration and alerting to Federal, State, and local agencies for critical infrastructure restoration when primary forms of communication are unavailable.

- HSIN-Critical Infrastructure (HSIN-CI) – Supports the exchange of threat information to critical infrastructure owners and operators in a variety of industries and locations, first responders and local officials.

8.4.2 Operation Centers

Operation centers associated with the Nuclear Sector include the Homeland Security Operations Center (HSOC), the DNDO Joint Center for Global Connectivity (JCGC), the NRC Operations Center, FBI Strategic Information and Operations Center (SIOC), DOE Emergency Operations Center, and National Response Center. In the event of an emergency, the operation centers will work together to address the matter. For instance, the NRC will provide staffing to the HSOC and the SIOC during incident response operations, and the DOE Emergency Operations Center will work with both DHS and NRC to monitor and direct the DOE emergency response assets during radiological incident response operations.

8.4.2.1 Homeland Security Operations Center (HSOC)

The HSOC serves as the Nation's hub for information sharing, situational awareness, and domestic incident management—increasing coordination among Federal, State, Territorial, local, tribal, and private sector partners, as well as select members of the international community. The HSOC houses representatives from more than 35 agencies, ranging from State and local law enforcement to Federal intelligence agencies, each supporting and contributing to the vital information sharing and coordination functions of the center. The HSOC monitors vulnerabilities and evaluates them against threats, providing a centralized real-time flow of information between Homeland Security partners. The HSOC will remain in constant communication with the White House, acting as the situational awareness conduit for the White House Situation Room by providing information needed to make decisions and define courses of action. During elevated threat conditions, the NSCC will participate in teleconference led by the DHS Assistant Secretary of Infrastructure Protection. The National Infrastructure Coordinating Center (NICC), an extension of the HSOC, is a 24/7, year round watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. The NICC provides a centralized mechanism and process for information sharing and coordination between and among government, SCCs, GCCs, and other industry partners. The NICC will share and coordinate information on: Alerts and Warnings; Suspicious Activity and Potential Threat Reporting; Incidents and Events; and National Response Planning & Execution.

DRAFT

8.4.2.2 DNDO Joint Center for Global Connectivity (JCGC)

The DNDO is presently in the process of establishing the Joint Center for Global Connectivity (JCGC). The JCGC will enhance the effective sharing and use of nuclear detection information and intelligence from all mission related detection systems to provide a greater situational awareness of the nuclear and radiological threat. By fusing the international and domestic detection streams and information generated by the intelligence and counterterrorism communities, the JCGC will be able to provide a better-informed decision making environment, enabling more effective alarm resolution, trend analysis, and threat awareness. Additionally, this information and analysis capability will be integrated with a detailed understanding of current and future detection system performance to increase our awareness and confidence in the global detection architecture.

8.4.2.3 NRC Operations Center

The NRC Operations Center staff is on duty 24 hours per day to serve as the focus point for communications, analysis, and response in support of State and local agencies during an emergency involving a U.S. commercial nuclear power plant, research, training or test reactor, fuel cycle facility, or nuclear materials licensee. The Headquarters Operations Officer (HOO) receives event reports and emergency declaration notifications. The HOO performs an initial assessment of the safety significance of each report based on extensive technical training, experience, agency guidance, and procedures. These reports may come from NRC licensees, State agencies that regulate Agreement State licensees, security and law enforcement personnel, contractors, military facilities, other government agencies (U.S. or foreign) or private citizens. Event and routine reports are maintained in databases, and posted to the NRC Web site on a daily basis. Security reports are also maintained in a database, but are only shared with select personnel at the NRC, the licensees and other State and Federal agencies. Significant events occurring at nuclear facilities that could potentially affect the public require activation of the NRC's Incident Response Plan, and prompt notifications to other Federal agencies, including DHS. These events can be related to a plant accident involving equipment malfunction or operator error that could lead to a potential radioactive release. They can also be due to an increase in the licensee's security posture due to some real or perceived threat to the facility. In addition to reporting actual events, facilities routinely contact the NRC Operations Center to conduct communications testing.

8.4.2.4 Strategic Information and Operations Center (SIOC)

The Strategic Information and Operations Center (SIOC) serves as the FBI's 24-hour clearinghouse for strategic information, and the center for crisis management and special event monitoring. The principal duties and responsibilities of the Center include its function as the FBI's central entity for the 24-hour collection and dissemination of strategic information. This is done through the SIOC Watch, which is operated on a 24/7, year round basis and consists of a minimum of two Supervisory Special Agents (Watch Supervisors) and three Emergency Action Specialists (EAS). This core group is joined by a representative from the National Security Agency, one to two members of the SIOC Information Support Group (SISG), an electronic technician and one or more information technology specialists. In the event of an incident at a nuclear power plant, the Nuclear Regulatory Commission will provide a liaison representative to the SIOC staff.

The watch teams on duty in the SIOC identify and assess potential emergency situations, and decide on follow-up measures, in accordance with standard operating procedures and

DRAFT

operational checklists. They assist and advise field offices and Legal Attaché Offices (LEGATS) after hours and on weekends on operational and informational matters. They facilitate the flow of information between the field and headquarters (HQ) executives, substantive units, and other government agencies and provide other support to FBI Executive Management and LEGATS as needed. They publish and post the SIOC Sentinel and the SIOC Morning Report to the SIOC Home Page on the FBI Intranet, Monday through Friday.

The staff is charged with maintaining the physical facilities, information systems, and communications equipment resident in the Center that facilitates the effective monitoring, coordination, and/or management of special events and critical incidents. The SIOC with its watch teams aids HQ investigative divisions in maintaining operational oversight of high-interest incidents and events, assists the protection details that ensure the security of the Attorney General, the Director of the FBI, and their families and serves as the communications focal point for the Director while on travel.

8.4.2.5 DOE Emergency Operations Center

The DOE Emergency Operations Center (EOC) functions as the DOE focal point for collecting, receiving, and disseminating essential information about emergencies, situations, incidents, or events affecting Departmental facilities, sites, programs, operations, and activities. It coordinates requests for usage of support for Departmental national emergency response assets and capabilities. In addition, the EOC supports classified and unclassified-level emergency response operations and requirements and facilitates inter- and intra-Departmental interfaces relating to emergency response operations, coordination, and information exchange. The EOC is staffed on a 24/7, year round basis with access to various secure and non-secure IT and physical resources, equipment, communications systems/networks, etc.

8.4.2.6 National Response Center

The primary function of the National Response Center[29] is to serve as a national point of contact for reporting all radiological, chemical, biological, oil, and etiological discharges into the environment anywhere in the United States and its territories. The National Response Center is staffed on a 24/7, year round basis by USCG personnel. In addition to gathering and distributing spill data for Federal On-Scene Coordinators and serving as the communications and operations center for the National Response Team, the National Response Center maintains agreements with a variety of federal entities to make additional notifications regarding incidents meeting established trigger criteria. For the Nuclear Regulatory Commission and DOE, the National Response Center makes telephonic notification of all incidents involving radioactive material releases to the environment.

The National Response Center also takes Terrorist/Suspicious Activity Reports and Maritime Security Breach Reports. The National Response Center established the Domestic Preparedness Chemical/Biological Hotline in conjunction with DOD and DOJ. The National Response Center takes reports via the toll-free numbers (1-877-24-WATCH or 1-800-424-8802)

[29] The acronym for the National Response Center is NRC. Because the acronym for the Nuclear Regulatory Commission is also NRC, the NRC acronym will not be used in this document for the National Response Center. In this document, the NRC acronym represents the Nuclear Regulatory Commission, and the National Response Center will be referred to by its full name.

on any incident related to potential or actual domestic terrorism and coordinates notifications and response with the FBI and the Soldier and Biological Chemical Command (SBCCOM).

DRAFT

List of Acronyms and Abbreviations

ACMUI	Advisory Committee on the Medical Uses of Isotopes
ACNW	Advisory Committee of Nuclear Waste
ACRS	Advisory Committee on Reactor Safeguards
AEA	Atomic Energy Act
AEC	Atomic Energy Commission
AMS	Aerial Measuring System
AOR	Area of Responsibility
ASLBP	Atomic Safety and Licensing Board Panel
ASM	Additional Security Measures
ASME	American Society of Mechanical Engineers
BCIS	Bureau of Citizenship and Immigration Services
BZPP	Buffer Zone Protection Plan
CBP	Bureau of Customs and Border Protection
CDA	Critical Digital Asset
CFR	Code of Federal Regulations
CII Act	Critical Infrastructure Information Act of 2002
CI/KR	Critical Infrastructure/Key Resource
CIP	Critical Infrastructure Protection
CNPPD	Chemical and Nuclear Preparedness and Protection Division
CR	Comprehensive Review
CRCPD	Conference of Radiation Control Program Directors
CWIN	Critical Infrastructure Warning Information Network
DBT	Design Basis Threat
DCS	Distributed Control Systems
DEST	Domestic Emergency Support Team
DHS	Department of Homeland Security
DHS-SAVE	DHS's Security Systematic Alien Verification for Entitlements
DNDO	Domestic Nuclear Detection Office
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State

DRAFT

1	DOT	Department of Transportation
2	EM/ER	Emergency Medical and Emergency Response
3	EMS	Emergency Medical Services
4	EP	Emergency Planning
5	EPA	Environmental Protection Agency
6	EPRI	Electric Power Research Institute
7	EPZ	Emergency Planning Zone
8	FBI	Federal Bureau of Investigation
9	FCC	Federal Communications Commission
10	FDA	Food and Drug Administration
11	FEMA	Federal Emergency Management Agency
12	FFD	Fitness-for-Duty
13	FR	Federal Register
14	FRMAC	Federal Radiological Monitoring and Assessment Center
15	FRPCC	Federal Radiological Policy Coordinating Committee
16	FY	Fiscal Year
17	GCC	Government Coordinating Council
18	GDP	Gaseous Diffusion Plant
19	GETS	Government Emergency Telecommunications Service
20	GPS	Global Positioning System
21	GTCC	Greater Than Class C
22	HHS	Health and Human Services
23	HQ	Headquarters
24	HSAS	Homeland Security Advisory System
25	HSC	Homeland Security Council
26	HSIN	Homeland Security Information Network
27	HSIN-CI	Homeland Security Information Network – Critical Infrastructure
28	HSOC	Homeland Security Operations Center
29	HSPD-7	Homeland Security Presidential Directive 7
30	I&C	Instrumentation and Control
31	IAEA	International Atomic Energy Agency
32	IAEA TECDOC	IAEA Technical Document
33	IMPEP	Integrated Materials Performance Evaluation Program
34	IND	Improvised Nuclear Device

DRAFT

1	INPO	Institute of Nuclear Power Operations
2	INSServ	International Nuclear Security Advisory Service
3	IPD	Infrastructure Partnerships Division
4	IPPAS	International Physical Protection Advisory Service
5	ISFSI	Independent Spent Fuel Storage Installation
6	ISL	In situ leach
7	JCATS	Joint Conflict and Tactical Simulation
8	LEGATS	Legal Attaché Offices
9	LLEA	Local Law Enforcement Agency
10	LLE	Local Law Enforcement
11	LLW	Low-Level Waste
12	MC&A	Material Control and Accounting
13	MOA	Memorandum of Agreement
14	MTSA	Marine Transportation Security Act
15	MW	Megawatts
16	NADB	National Asset Database
17	NAICS	North American Industry Classification System
18	NARAC	National Atmospheric Release Advisory Center
19	NCS	National Communications System
20	NEA	Nuclear Energy Agency
21	NEI	Nuclear Energy Institute
22	NICC	National Infrastructure Coordination Center
23	NIMS	National Incident Management System
24	NIPP	National Infrastructure Protection Plan
25	NMMSS	Nuclear Materials Management and Safeguards System
26	NNSA	National Nuclear Security Administration
27	NORM	Naturally Occurring Radioactive Material
28	NRC	Nuclear Regulatory Commission
29	NRP	National Response Plan
30	NSI	National Security Information
31	NSCC	Nuclear Sector Coordinating Council
32	NSCC-R	Nuclear Sector Coordinating Council – Radioisotopes Subcouncil
33	NUREG	United States Nuclear Regulatory Commission Regulation
34	OAS	Organization of Agreement States

DRAFT

OECD	Organization for Economic Co-operation and Development
OSHA	Occupational Safety and Health Administration
OSRP	Offsite Source Recovery Program
OSTP	Office of Science and Technology Policy
PCII	Protected Critical Infrastructure Information
PCS	Process Control Systems
PFS	Private Fuel Storage
PNNL	Pacific Northwest National Laboratory
PPSDP	Physical Protection Significance Determination Process
PRA	Probabilistic Risk Analysis
PSA	Protective Security Advisor
PSAT	Protective Security Advisory Team
R&D	Research and Development
RAMCAP	Risk Analysis and Management of Critical Assets Protection
RAMQC	Radiological Material Quantities of Concern
RAP	Radiological Assistance Program
RASCAL	Radiological Assessment System for Consequence Analysis
RaSSIA	Radiation Safety and Security of Radioactive Sources Infrastructure Appraisal
RD	Restricted Data
RDD	Radiological Dispersal Device
REAC/TS	Radiation Emergency Assistance Center/Training Site
RED	Radiological Exposure Device
RIS	Regulatory Issue Summary
RMD	Risk Management Division
RMP	Risk Management Plan
RTR	Research and Test Reactors
S&T	Science and Technology Directorate
SA	Security Assessment
SAC	Special Agent in Charge
SAV	Site Assistance Visit
SBCCOM	Soldier and Biological Chemical Command
SCADA	Supervisor Control and Data Acquisition
SER	Safety Evaluation Report
SFP	Spent Fuel Pool

DRAFT

SGI	Safeguards Information
SIOC	Strategic Information and Operations Center
SM	Source Material
SNF	Spent Nuclear Fuel
SNM	Special Nuclear Material
SRP	Standard Review Plan
SSA	Sector-Specific Agency
SSNM	Strategic Special Nuclear Material
SSP	Sector-Specific Plan
SSVNS	Social Security Number Verification System
SWG	Security Working Group
TAS	Threat Assessment Section
TRTR	National Organization for Test, Research, and Training Reactors
TSA	Transportation Security Administration
TSP	Telecommunications Service Priority
USC	United States Code
USCG	United States Coast Guard
USEC	United States Enrichment Corporation
WANO	World Association of Nuclear Operators
WMD	Weapons of Mass Destruction
WMD-CST	Weapons of Mass Destruction Civil Support Teams
WPS	Wireless Priority Service

DRAFT

Glossary of Terms

Byproduct material - Generally, nuclear material (other than special nuclear material) that is produced or made radioactive in a nuclear reactor. Also the tailings and waste produced by extraction or concentration of uranium or thorium from an ore processed primarily for its source material content.

Code of Federal Regulations (CFR) - The codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation. Each volume of the CFR is updated once each calendar year and is issued on a quarterly basis.

Nuclear facilities – A term that includes all facilities that are part of the nuclear sector, such as: commercial nuclear power plants; research and test reactors; nuclear fuel cycle facilities; radioactive waste management facilities; deactivated nuclear facilities; facilities housing radioactive materials; and radioactive source production and distribution facilities.

Nuclear material - Uranium, plutonium or another substance which is or may be used for extraction of nuclear energy (nuclear fuel), or a compound containing such a substance; thorium or another substance suited for conversion into nuclear fuel, or a compound containing such a substance; and spent nuclear fuel which has not been placed in final storage.

Radioactive Material - Material that undergoes spontaneous emission of radiation (alpha, particles, beta particles and gamma rays) directly from unstable atomic nuclei.

Radiological Exposure Device (RED) – A device whose purpose is to expose people to radiation, rather than to disperse radioactive material into the air, as would an RDD. An RED could be constructed from unshielded or partially shielded radioactive materials in any form placed in any type of container.

Radioactive materials in quantities of concern – Category 1 and 2 values in the IAEA Code of Conduct on Safety and Security of Radioactive Sources (July 2003).

Source material - Natural uranium or thorium or depleted uranium that is not suitable for use as reactor fuel

Special nuclear material - Uranium-233 or uranium-235, enriched uranium, or plutonium

Strategic special nuclear material - Uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium- 233, or plutonium.

DRAFT

Appendices

DRAFT

1 Authorities

Protection of the assets defined in this sector requires activities that entail a high level of cooperation and coordination among diverse entities in the public and private sectors. Numerous legal authorities govern these activities. These authorities are summarized below.

Department of Homeland Security

The Department of Homeland Security's authority is derived from the Homeland Security Act, Pub. L. 107-296, 116 Stat. 2135 (2002), and a number of Homeland Security Presidential Directives.

On December 17, 2003, the President issued HSPD-7, 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 attack." The Secretary of the Department of Homeland Security, in accordance with paragraph 29 of HSPD-7, will continue to work with the NRC and DOE in order to ensure the necessary protection of the assets described in this sector, including nuclear reactors, materials, and waste. In accordance with paragraph 25 of HSPD-7, DHS and sector-specific agencies will collaborate with appropriate private sector entities, and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and sector-specific agency shall collaborate with the private sector and continue to support sector coordinating mechanisms:

- To identify, prioritize, and coordinate the protection of critical infrastructure and key resources
- To facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices

On April 15, 2005, the President issued HSPD-14/NSPD-43, "Domestic Nuclear Detection". This Directive established the DNDO, within DHS to:

- Serve as the primary entity in the United States Government to further develop, acquire, and support the deployment of an enhanced domestic system to detect and report on attempts to import, possess, store, transport, develop, or use an unauthorized nuclear explosive device, fissile material, or radiological material in the United States, and improve that system over time;
- Enhance and coordinate the nuclear detection efforts of Federal, State, local, Territorial, and tribal governments and the private sector to ensure a managed, coordinated response;
- Establish, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of Defense and Energy, additional protocols and procedures for use within the United States to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to the Attorney General, the Secretaries of Defense, Homeland Security, and Energy, and other appropriate officials or their respective designees for appropriate action by law enforcement, military, emergency response, or other authorities;

DRAFT

- Develop, with the approval of the Secretary of Homeland Security and in coordination with the Attorney General and the Secretaries of State, Defense, and Energy, an enhanced global nuclear detection architecture with the following implementation: (i) the DNDO will be responsible for the implementation of the domestic portion of the global architecture; (ii) the Secretary of Defense will retain responsibility for implementation of DOD requirements within and outside the United States; and (iii) the Secretaries of State, Defense, and Energy will maintain their respective responsibilities for policy guidance and implementation of the portion of the global architecture outside the United States, which will be implemented consistent with applicable laws and relevant international arrangements;
- Conduct, support, coordinate, and encourage an aggressive, expedited, evolutionary, and transformational program of research and development efforts to support the policy set forth in paragraph (I);
- Support and enhance the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as provide appropriate information to these entities; and
- Further enhance and maintain continuous awareness by analyzing information from all DNDO mission-related detection systems.

On December 7, 1979, the President directed the Federal Emergency Management Agency (FEMA) to assume the lead responsibility for all offsite nuclear planning and response. FEMA's activities are conducted pursuant to 44 Code of Federal Regulations (CFR) Parts 350, 351, and 352. These regulations are a key element in the Radiological Emergency Preparedness (REP) Program established following the Three Mile Island Nuclear Power Station accident in March 1979.

FEMA Rule 44 CFR 350 establishes the policies and procedures for REP's initial and continued approval of tribal, State, and local governments' radiological emergency planning and preparedness for commercial nuclear power plants. This approval is contingent, in part, on State and local government participation in joint exercises with licensees.

REP's responsibilities in radiological emergency planning for fixed nuclear facilities include the following:

- Taking the lead in offsite emergency planning and in the review and evaluation of radiological emergency response plans (RERPs) and procedures developed by State and local governments;
- Determining whether such plans and procedures can be implemented on the basis of observation and evaluation of exercises of the plans and procedures conducted by State and local governments;
- Responding to requests by the U.S. Nuclear Regulatory Commission (NRC) pursuant to the Memorandum of Understanding between the NRC and FEMA dated June 17, 1993 (44 CFR Part 354, Appendix A, September 14, 1993); and
- Coordinating the activities of Federal agencies with responsibilities in the radiological emergency planning process through the Federal Radiological Preparedness Coordinating Committee (FRPCC) and the Regional Assistance Committee (RAC).

DRAFT

Department of Transportation

The Federal hazardous materials transportation law, 49 United States Code (USC) 5101 et seq. and pipeline safety law, 49 USC 60101 et seq. give the Secretary of Transportation the regulatory and enforcement authority to enhance the safe transportation of hazardous materials by all modes, and hazardous liquids and natural gas by pipeline. The Secretary of Transportation also has authority to marshal transportation in a defined area to aid in the national defense and homeland security, via the Defense Productions Act of 1950, 50 USC App.2071 and the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 USC 5121 et seq. In allocating or prioritizing civil transportation resources, the Secretary, with appropriate funding from one of three agencies (DOD, DOE, or DHS) has extensive authority, in all modes, to organize transportation in the event of an emergency. Also the Homeland Security Act of 2002 amended the Federal hazardous materials transportation law, 49 USC 5103 to include security, so the mandate now reads that the Secretary of Transportation "prescribe regulations for the safe transportation, including security, of hazardous materials in intrastate, interstate, and foreign commerce."

Nuclear Regulatory Commission

The Atomic Energy Act of 1954, as amended, is the primary source of the NRC's authority to regulate radioactive materials and civilian nuclear activities. NRC regulations are set forth in Title 10 of the CFR, Energy, Parts 0-199.

The NRC and its licensees share a common responsibility to protect public health and safety; Federal regulations and the NRC regulatory program are important elements in the protection of the public. NRC licensees, however, have the day-to-day responsibility for ensuring the safe use of nuclear materials.

The following principal statutory authorities govern the NRC's work:

- **Atomic Energy Act of 1954, as amended (AEA):** Under the AEA, the NRC has broad authority to regulate (by regulation, licensing or order) the possession, transfer, and use of source, byproduct, and special nuclear material to protect the public health and safety and to provide for the common defense and security. Under AEA § 147, 42 USC 2167, the NRC also has the authority to designate information as "Safeguards Information" (SGI) to prevent its unauthorized disclosure.
- **Energy Reorganization Act of 1974:** This act abolished the Atomic Energy Commission (AEC) and moved the AEC's regulatory function to the NRC, establishing the NRC as an independent regulator of certain nuclear materials and facilities. The act also created what eventually became the DOE. The DOE addresses military uses of AEA material, as well as nuclear energy research. Unless specifically authorized by legislation, NRC does not regulate DOE activities, which includes the promotion of nuclear energy and development of nuclear materials for military uses.

Other statutes that form the basis of NRC regulatory authority:

- **Energy Policy Act of 2005:** As part of the Energy Policy Act, the NRC is required to conduct security evaluations, including force-on-force exercises not less than once every

DRAFT

three years at licensed commercial power reactor facilities; the Design Basis Threat (DBT) will include rulemaking and public comment; the NRC must assign a Federal security coordinator employed by the NRC in each region; requires NRC to promulgate regulations establishing a mandatory tracking system for radiation sources in the U.S.; establishes a task force on Radiation Source Protection and Security to evaluate and provide recommendations to Congress and the President on security of radiation sources in the U.S. from potential threats; expands the scope of fingerprinting and criminal history checks at licensee facilities; in coordination with the Department of Justice, allows for a broader class of weapons to be used to protect NRC-licensed or certified facilities or materials; expands criminal sanctions for sabotage of nuclear facilities, fuel or material; expands the provisions for unlawful trespass with dangerous weapons, explosives, and other dangerous instruments at NRC-licensed and NRC-certified facilities; and requires the NRC to consult with DHS regarding the proposed location of new utilization facilities.

- **Uranium Mill Tailings Radiation Control Act of 1978:** This act regulates uranium mill tailings and any remediation that might be associated with the mill sites.
- **Nuclear Non-Proliferation Act of 1978:** This act (in combination with the AEA) gives the NRC authority to license the export and import of nuclear materials and equipment to ensure that these items are used for peaceful purposes. For all nuclear exports, the NRC must find that the export will not be "inimical to the common defense and security." No commercial export license for nuclear facilities, source material, or special nuclear material may be issued by the NRC unless the United States Government and the country of export have in place an agreement for cooperation meeting the requirements of AEA § 123, 42 USC § 10143.
- **Nuclear Waste Policy Act of 1982/Nuclear Waste Policy Act Amendments of 1987/Energy Policy Act of 1992:** These acts, in combination, set forth requirements for the development and licensing of Yucca Mountain, a proposed high-level radioactive waste repository being developed by DOE. In contrast to the NRC's legislatively mandated authority to regulate disposal, NRC's ability to regulate transportation to the repository is specifically limited by the Nuclear Waste Policy Act, as amended, to the certification of transportation packages and the prenotification of shipments.
- **Diplomatic Security and Anti-Terrorism Act of 1986:** This act requires the Secretaries of Defense, State, and Energy, and the NRC to review the adequacy of the physical security standards currently applicable to the shipment and storage outside the United States of special nuclear material which is subject to U.S. prior-consent rights, with special attention to protection against terrorist acts. The act also requires these officials and the NRC to report to specified congressional committees on the results of such review.

The act also amends the AEA to require each licensee or applicant for a license to operate a utilization facility (e.g., a nuclear power reactor) to fingerprint each individual who is permitted unescorted access to the facility, or is permitted access to certain Safeguards Information. The act provides that all fingerprints shall be submitted to the Attorney General for identification and a criminal history records check, with all costs to be paid by the licensee or applicant.

DRAFT

- **Solar, Wind, Waste, and Geothermal Power Production Incentives Act of 1990**: This act amended the AEA to require licensing of uranium enrichment facilities, other than existing gaseous diffusion plants.

Federal Bureau of Investigation (FBI)

In addition to the FBI's overarching terrorism response authorities as outlined in various National Security and Homeland Security Presidential Directives, the following statutes apply specifically to the FBI's enforcement of statutes aimed at preventing criminal/terrorist activity involving nuclear/radiological materials:

- Atomic Energy Act (42 USC 2011-2284)
- 18 USC 831 (Prohibited Transactions Involving Nuclear Materials)
- 18 USC 832 (Participation in Nuclear and Weapons of Mass Destruction (WMD) Threats to the United States)
- 18 USC 2332a (Weapons of Mass Destruction Statute)

As also stated in the National Response Plan (NRP), the Attorney General, generally acting through the FBI, has lead responsibility for criminal investigations of terrorist acts or terrorist threats and for coordinating activities of other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt terrorist attacks against the United States, including incidents involving nuclear/radioactive materials.

DRAFT

2 Sector Protective Programs

Initiatives

Integrated Response

To promote better communication of protective program issues between the NRC and its stakeholders, the NRC and DHS are coordinating State and local outreach efforts and exercise participation initiatives to:

- Promote consistency
- Promote participation in more national-level exercises
- Encourage revisions of State and local plans and procedures in order for them to be aligned with the NRP
- Integrate the National Incident Management System (NIMS) into current State and local concepts of operations

Reactors and Spent Fuel Facilities

The following sector initiatives contribute to enhancing commercial reactor plant and spent fuel facility security:

- The owner/operators of commercial nuclear power plants undertook an initiative to review the vulnerabilities and mitigation measures for spent fuel pools. This initiative was completed in September 2005. The results will be reviewed by a panel of industry experts and recommendations for implementation of additional measures provided to the owner/operators.
- The NRC has urged its licensees to use Federal government databases to help prevent the use of fraudulent documentation for gaining access to nuclear facilities. The Social Security Administration's web-based Social Security Number Verification System (SSNVS), and DHS's Security Systematic Alien Verification for Entitlements (DHS-SAVE), which verifies the immigration status of non-citizens, are two examples of this information sharing initiative.
- The NRC is requiring expanded, expedited, and more-thorough background checks for nuclear power plant employees to ensure that they are reliable and trustworthy.
- The NRC, as part of its comprehensive security program, is increasing the frequency and fidelity of force-on-force exercises at power reactor sites and Category I fuel cycle facilities. The NRC has regularly carried out force-on-force exercises at operating nuclear power plants since the 1980s. Force-on-force exercises are conducted to assess and improve, as necessary, the performance of defensive strategies at licensed facilities. These exercises are intended to be a primary means to conduct performance-based testing of a licensee's security force, and its ability to prevent radiological sabotage, as required by NRC regulations (10 CFR Part 73). Force-on-force exercises are also part of a robust network of the NRC's security oversight program.
- The full force-on-force exercise, which includes onsite tabletop and force-on-force exercises, is conducted over several days. First, NRC security, emergency

DRAFT

preparedness, and operations specialists conduct tabletop exercises in which they evaluate the effectiveness of the licensee security plans against a series of attack scenarios. The role of Federal, State, and local law enforcement and emergency management officials is also discussed in this phase of the exercise. In the second phase, armed with information from the tabletops, and with information gathered prior to the tabletops, detailed plans are made for a number of commando-style attacks seeking to probe for potential deficiencies in the defensive strategy.

- The NRC has required enhanced training and qualifications for security personnel at nuclear power plants, especially in tactical response. This includes more frequent firing of weapons, more realistic training under different conditions, and firing against moving and fixed targets. To minimize security personnel fatigue, the NRC established detailed requirements for a 48-hour work week, except for special circumstances, and limits on the amount of overtime that guards can work.
- In addition to requiring licensees to implement additional protective measures, the NRC is responding to the terrorist threat in a comprehensive fashion. The NRC has undertaken a comprehensive re-evaluation of its safeguards and security program, regulations, and procedures that has resulted in numerous security improvements. As part of this program review, the NRC has made interim revisions to the DBTs, and is moving towards a formal rulemaking to make these and other revisions permanent.
- The NRC is supporting DHS and the Homeland Security Council (HSC) to conduct tabletop exercises aimed at enhancing integrated response planning and exploring coordinated response by local, State and Federal agencies.
- The NRC is also working with appropriate Federal agencies to assess and respond to potential airborne threats. For example, the NRC has worked with the Federal Aviation Administration and DOD to put in place a notice to airmen, advising pilots not to circle or loiter above nuclear power plants and other nuclear facilities. If they ignore the notice, they can expect to be interviewed by law enforcement personnel.
- Congress recently enacted in the Energy Policy Act of 2005 provisions that will further enhance security of NRC-licensed activities. One provision will allow the NRC, in consultation with the Attorney General, to authorize guards at NRC-designated facilities the authority to possess or use weapons comparable with those used by the DOE's guard forces. Another provision will make it a Federal crime to bring unauthorized weapons and explosives into NRC-licensed facilities. The NRC will also expand Federal prohibitions on sabotage applicable to the operation and construction of certain nuclear facilities and materials. In addition, the NRC has been given authority to require fingerprinting and criminal checks of broader categories of licensee employees who have access to radioactive material or safeguards information.
- DHS/SSA is in the process of implementing the BZPP within this sector. The BZPP establishes a protection zone outside the licensees' property in which LLEA will seek to identify and deter any security threat to the infrastructure asset.
- Department of Homeland Security is coordinating potential integrated response enhancements, building on pilot exercises conducted at two power reactor facilities.
- The commercial nuclear power plants have developed a close working relationship with local law enforcement and local offices of the Federal law enforcement agencies through integrated emergency planning beyond those initiated by power plant events. Coordination during natural disasters such as hurricanes, tornadoes, flooding and other

DRAFT

industry initiated events has established strong lines of communication. Further, the facilities at commercial nuclear power plants, such as firing ranges, are generally superior to local available facilities and, therefore, are offered to the law enforcement agencies for their use. Since 9/11, local law enforcement has increased their presence at commercial nuclear power plants as a visual deterrent to terrorism.

- The comprehensive review process that will be performed at every commercial nuclear power plant is providing another avenue for further cooperation among off-site agencies and the power plant security force. Solving problems of communications between agencies and the power plant security groups increases the opportunity for interaction and real-time sharing of information.

Radioactive materials in quantities of concern

The NRC, States, and the nuclear industry have taken a number of actions to ensure the safe operation of nuclear facilities that possess and use radiological materials. The following information outlines the NRC's protective program plan for risk-significant radioactive sources licensed by the NRC for medical, industrial, and academic uses. It includes actions that are completed, under way, or planned, to enhance security and safety controls for the materials of concern for use in RDDs:

- The NRC is coordinating with DOE and DOS to work with the IAEA to encourage member States to participate in the model projects on upgrading radiation protection infrastructure and other programs that enhance cradle-to-grave national regulatory safety and security controls over radioactive sources.
- The NRC has started the development of mechanisms to track radioactive material of greatest concern through all phases of use and disposition, to include tagging sources, database development and accessibility, and tracking capabilities. DHS, NRC, DOE, and other Agencies are cooperating on the development of a National Source Tracking System. The information in the system will be protected.
- The NRC will continue to leverage technology in its efforts to protect radioactive materials in quantities of concern from theft and diversion. Systems are being considered that will enhance the ability of materials shippers to accurately track the status of risk-significant shipments using satellite tracking systems, and other state-of-the-art technologies.
- The NRC is in the process of establishing the mechanisms for verifying the legitimacy of licensees via an accessible database, to include NRC and Agreement State licensees. This will allow a licensee that is transferring licensed material to verify that the recipient is licensed to possess the material, thereby mitigating the vulnerability of fraudulent license documents being used to acquire radioactive material.
- The NRC is developing and implementing inspections and enforcement protocols for security requirements of radioactive materials in quantities of concern.
- The NRC is participating in the development and incorporation of security standards into IAEA's transportation guidelines.
- The NRC is participating in an international working group that is addressing sabotage concerns for transport and shipping casks.

DRAFT

- The NRC coordinated with DHS and States to implement security enhancements for non-AEA (i.e., naturally occurring) radiological material of concern for use in RDDs. Ultimately, Section 651 (e) of the Energy Policy Act of 2005 expanded the definition of byproduct material in Section 11 e. of the Atomic Energy Act of 1954 to include certain naturally-occurring and accelerator-produced radioactive materials (NARM). The NRC is coordinating this issue with the States to develop a consistent nationwide regulatory framework for the safety and security of these radioactive materials. The NRC considers cyber security issues, as appropriate for materials facilities, as part of its ongoing vulnerability assessment program.
- DHS, NRC, and DOE are expanding the existing offsite source recovery program (OSRP) program to identify, collect, and dispose of stolen, lost, and orphaned sources, to include unwanted or end-of-life radioactive materials of concern.
- The NRC is coordinating with DOE, other Federal agencies, the Conference of Radiation Control Program Directors (CRCPD), and individual States to establish a strategy for storage/disposal of radioactive materials in quantities of concern.
- The NRC continues to coordinate with and fund CRCPD to implement and further develop its national orphan source program.
- The NRC is working with DOE, other Federal agencies, and States to assure proper and secure disposal of sources at end of life, including GTCC sources.
- DHS is undertaking an enhancement of the ability of local public safety personnel to detect radioactive materials that may have escaped the control of their owners, for possible use in a WMD.

DHS is coordinating with Improvised Nuclear Device (IND)/RDD working group efforts. The DHS IND/RDD Phase II Working Group consists of all Federal agencies working together (with DHS as chair of six subgroups) to prepare policy options to prevent terrorist introduction or use of nuclear and/or radiological devices and material within the United States through detection, interdiction, neutralization, and disposal of such devices, and to respond quickly in the aftermath of a domestic and/or nuclear event. The HSC is coordinating similar efforts to combat nuclear and radiological terrorism that crosscut numerous Agencies.

Information Security

The staff has introduced a rule making to enhance the measures concerning access authorization, handling, and protection of Safeguards Information as it pertains to licensees. Other steps include computerized training for users/designators and a designation guide to facilitate improved understanding of what is Safeguards Information. Subject matter experts have assisted counterparts in other Federal agencies in order to provide protection for such information and ensure proper handling. Some of the ways that information can be protected includes the Protected Critical Infrastructure Information (PCII) Program, categorizing information as Safeguards Information (SGI), and classifying information. More information about protecting information can be found in Section 3.4.

The NRC continues to be involved in ensuring that the appropriate balance exists between the sensitivity of information and the right of the public to be informed about NRC actions and decisions. To that end, NRC formed a Task Force on Public Disclosure and Security-Related Information. The existence of the Task Force, as well as current NRC posture, have been made publicly available.

DRAFT

1

DRAFT