Regulatory Analysis and Backfit Analysis

Final Rulemaking:
Power Reactor Security Requirements

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Office of Nuclear Security and Incident Response

Table of Contents

Executive Summary

The Nuclear Regulatory Commission (NRC) is amending the current security regulations and adding new security requirements pertaining to nuclear power reactors. The rulemaking: (1) makes generically applicable many of the security requirements imposed by Commission orders issued after the terrorist attacks of September 11, 2001, (2) adds several new requirements that resulted from insights gained while implementing the security orders, reviewing site security plans, and implementing the enhanced baseline inspection program and force-on-force exercises, (3) updates the regulatory framework in preparation for receiving license applications for new reactors, (4) imposes requirements to assess and manage site activities that can adversely affect safety and security, and (5) considered three petitions for rulemaking (PRM) as part of the effort to develop the security requirements. The safety and security requirements (in § 73.58) address, in part, PRM-50-80 that requested the establishment of regulations governing changes to facilities which could adversely affect the protection against radiological sabotage. The other two PRMs considered as part of this rulemaking were PRM-73-11 and PRM-73-13.

Several significant changes to this rulemaking occurred after the proposed rule stage. The final power reactor security rule does not contain the weapons provisions (§§ 73.18 and 73.19) and the reporting provisions (§ 73.71 and appendix G to part 73) that were included as part of the proposed rule. These provisions are being addressed in a separate rulemaking. Additionally, the cyber requirements that were in proposed § 73.55 were moved to a stand-alone section within part 73: § 73.54. Requirements stemming from section B.5 of the 2002 Interim Compensatory Measures (EA-02-026) order (regarding licensee procedures for responding to notifications of potential aircraft threats and for developing guidance and strategies to address the loss of large areas of the plant due to explosions or fires from a beyond-design basis event), that were contained in proposed appendix C to part 73, have been moved to 10 CFR 50.54(hh) and were republished as a supplemental proposed rule in April 10, 2008 (73 FR 19443). The proposed § 73.2 definitions (most of which applied to the proposed weapons provisions in §§ 73.18 and 73.19) that remain applicable are no longer in the final rule, and instead will be addressed in supporting guidance.

The analysis presented in this document examines the benefits and costs of the final security requirements relative to the baseline of existing security requirements, including current regulations and the relevant orders. The key findings of the analysis are as follows:

- Total Cost to Industry. The final rule will result in a total one-time cost to all nuclear power plant sites of approximately $115.71 million, followed by total annual costs on the order of $38.65 million. The total present value of these costs is estimated at $590.23 million (using a 7-percent discount rate) and $857.33 million (using a 3-percent discount rate) over the next 30 years.

- Average Cost per Site. The average nuclear power plant site, which may include multiple units, will incur a one-time cost of approximately $1.78 million followed by annual costs of approximately $594,600.

- Annual Impact to the Economy. The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these "annualized" one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

- Value of Benefits Not Reflected Above. With the exception of some of the direct monetary savings to industry, the cost figures shown above do not reflect the value of the benefits of the final rule. These benefits are evaluated qualitatively in Section 4.1. This regulatory analysis concluded the costs of the rule are justified in view of the qualitative benefits.

- Costs to NRC. The rule will result in a one-time cost to NRC of approximately $2.60 million. NRC is not expected to incur substantial annual costs as a result of the rule.

- Decision Rationale. Although the NRC did not quantify the benefits of this rule, the staff did qualitatively examine benefits and concluded that the rule will provide safety and security-related benefits. The sum total of the requirements in the final rule will provide additional assurance of licensees' capabilities to protect power reactor sites against an assault as defined by the DBT of radiological sabotage. Specifically, the final rule will require that a single act of radiological sabotage cannot simultaneously disable the function of both CAS and SAS. The rule also requires certain electronic equipment used for alarms and communications to have uninterruptible backup power. The final rule will result in the deployment of certain technological advances in intrusion detection systems that are necessary during a safeguards contingency event. In recognition of advancing digital technology, the final rule will maintain the intent of the security orders by establishing the requirement for a cyber security program to protect any systems that, if compromised, could adversely impact safety, security or emergency preparedness. The final rule will increase licensees' security programs' effectiveness through additional training and procedures such as safety/security interface, on-the-job training, and recurring criminal and credit history checks, and psychological assessments. The final rule access authorization amendments will improve the integration of the access authorization requirements, fitness-for-duty requirements, and security program requirements by increasing the rigor for some elements of the access authorization program, developing procedures to provide communication between a licensed psychologist or psychiatrist and other medical personnel, and adding requirements that subject additional individuals (such as those who have electronic access via computer systems or those who administer the access authorization program) to the access authorization requirements. NRC believes that these factors represent a substantial increase in safety and that the costs of the final rulemaking are justified based on these qualitative benefits.

The rule requirements will apply to new reactors, including Watts Bar Unit 2 (although it is important to note that Watts Bar Unit 2 is specifically required to meet the requirements applicable to current licensees) and any units that would be built under the new reactor applications that NRC has received to date. Because security program costs are largely a site-

based function, rather than a reactor-based function, the regulatory analysis and backfit analysis reflect costs associated with the co-located new reactors (currently that is Watts Bar Unit 2 and seven of the nine applications). For the new reactor applications that would place new reactors at sites that are not co-located (currently two applications) with operating reactors, this analysis estimates that one-time and annual impacts will be less than or equal to the corresponding impacts for operating reactors (i.e., because the development of security plans and systems for the new sites will not require that existing plans and systems be analyzed and reworked). However, the quantitative results do not reflect any additional incremental cost for the non-co-located reactors due to the uncertainty associated with when and if these facilities actually will be licensed and operated.

Abbreviations

AA	Access Authorization
DBT	Design Basis Threat
CAS	Central Alarm Station
CFR	Code of Federal Regulations
CRGR	Committee to Review Generic Requirements
DBT	Design-Basis Threat
ICM	Interim Compensatory Measure
NRC	Nuclear Regulatory Commission
OCA	Owner Controlled Area
PA	Protected Area
PRM	Petition for Rulemaking
SAS	Secondary Alarm Station
UCS	Union of Concerned Scientists

1. Introduction

This document presents a regulatory analysis of final revisions to the power reactor security requirements as set forth by the U.S. Nuclear Regulatory Commission (NRC) in Title 10, part 73, of the Code of Federal Regulations (10 CFR part 73). This introduction is divided into three sections. Section 1.1 states the problem and the reasons for the final rulemaking, Section 1.2 provides background information on the power reactor security rulemaking, and Section 1.3 discusses regulatory objectives related to adoption of the final revisions to the power reactor security rulemaking.

1.1 Statement of the Problem and Reasons for the Rulemaking

Following the terrorist attacks that occurred 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 given the changing threat environment. Through a series of orders, the Commission specified a supplement to the Design Basis Threat (DBT), as well as requirements for specific training enhancements, access authorization enhancements, security officer work hours, and enhancements to defensive strategies, mitigative measures, and integrated response. Additionally, in generic communications, the Commission specified expectations for enhanced notifications to the NRC for certain security events or suspicious activities.

While those specific requirements are Safeguards Information (SGI), in general the changes 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.

The NRC, in implementing the security orders, reviewing the revised site security plans across the fleet of reactors, conducting the enhanced baseline inspection program, and evaluating force-on-force exercises, identified additional security measures that would provide added assurance of licensees' capability to protect against the DBT.

In addition, three petitions for rulemaking (PRMs) were addressed or considered as part of this rulemaking. PRM-50-80, submitted by David Lochbaum on behalf of the Union of Concerned Scientists (UCS) and San Luis Obispo Mothers for Peace, requested the establishment of regulations governing changes to facilities which could adversely affect their protection against radiological sabotage. This petition was partially granted on November 17, 2005 (70 FR 69690), and the new § 73.58 "Safety/security interface requirements for nuclear power reactors" contains requirements to address this aspect of the petition. PRM-73-11, submitted by Scott Portzline on behalf of Three Mile Island Alert, requested that the regulations governing physical

security be amended to require armed guards at the entrances to the owner controlled areas. This request was considered as part of the development of the final § 73.55 requirements. However, contrary to the request, the NRC is not requiring armed guards at the entrances of the owner controlled area as discussed in section II of the final rule Federal Register notice. Finally, PRM-73-13, submitted by David Lochbaum on behalf of UCS, requested that the requirements governing escort within, and access to, the protected area of the power reactor facility be amended to require armed escorts and to deny access to the protected area for individuals for which information becomes known that would prevent such an individual from gaining unescorted access. This PRM was considered as part of the effort to finalize both the § 73.56 and § 73.55 requirements. The NRC is not adopting either of the recommendations of the petition as discussed in section II of the final rule Federal Register notice.

1.2 Background

1.2.1 Current Regulations Governing Power Reactor Security (10 CFR Part 73)

NRC's regulatory requirements for the physical protection of plants and materials are contained in 10 CFR part 73. Part 73 distinguishes between requirements applicable to power reactors and to special nuclear material at fixed sites and in transit. Requirements for fixed sites vary depending on the type of site and the relevant DBT as described in § 73.1(a). The physical protection requirements for nuclear power reactors are contained in § 73.55 and focus on protecting against the DBT of radiological sabotage.

To protect against this DBT, the current requirements in § 73.55 that this rule will amend begin by establishing the following general objective (§ 73.55(a)):

> The licensee shall establish and maintain an onsite physical protection system and security organization which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The physical protection system shall be designed to protect against the design basis threat of radiological sabotage as stated in § 73.1(a).

In the current §§ 73.55(b)-(h) that this final rule will amend, the regulation establishes detailed requirements addressing the following aspects of licensees' physical protection systems:

- Physical security organizations,
- Physical barriers,
- Access requirements,
- Detection aids,

- Communications,
- Testing and maintenance procedures, and
- Response requirements.

Some of the provisions within the paragraphs identified above are particularly relevant to this analysis and are briefly described or summarized below.

Security Plans

Under 10 CFR 50.34(c), applicants for an operating license for a production or utilization facility are required to develop a security plan for NRC review and approval. 10 CFR 73.55(b), paragraphs (1)(i) and (3)(i) require licensees to maintain safeguards in accordance with their security plans and procedures. The security plan describes how the licensee or applicant will meet the requirements of part 73 (including the requirements for barriers, access requirements, systems, and equipment as required in §§ 73.55(b)-(h)).

Safeguards Contingency Plans

Under 10 CFR 50.34(d), applicants for an operating license for a production or utilization facility are required to develop a safeguards contingency plan in accordance with the criteria set forth in appendix C to 10 CFR part 73. The safeguards contingency plan must include plans for protecting against threats, thefts, and radiological sabotage. Under § 73.55(h)(1), licensees must maintain and implement their NRC-approved safeguards contingency plan. In accordance with 10 CFR part 73, appendix C, the goals of this plan are (1) to organize the response effort at the licensee level, (2) to provide predetermined, structured responses by licensees to safeguards contingencies, (3) to ensure the integration of the licensee response with the responses by other entities, and (4) to achieve a measurable performance in response capability.

Training and Qualification Plan

Under § 73.55(b)(4)(ii), licensees are required to establish, maintain, and implement an NRC-approved training and qualification plan outlining the processes by which security personnel will be selected, trained, equipped, tested, and qualified in accordance with appendix B to 10 CFR part 73.

1.2.2 Commission Orders

The Commission imposed four security orders on all operating power reactor licensees following September 11, 2001:

- EA-02-026, "Interim Compensatory Measures (ICM) Order," dated February 25, 2002, 67 FR 9792 (March 4, 2002);

- EA-02-261, "Access Authorization Order," dated January 7, 2003, 68 FR 1643 (January 13, 2003);
- EA-03-039, "Security Personnel Training and Qualification Requirements (Training) Order," dated April 29, 2003, 68 FR 24514 (May 7, 2003); and
- EA-03-086, “Revised Design Basis Threat Order,” dated April 29, 2003, 68 FR 24517 (May 7, 2003).

The specifics of the security changes contained in the security orders are controlled as SGI per § 73.21 but some of the general security enhancements are discussed briefly. The “ICM Order” required licenses to implement various security actions, such as: review and update the security and emergency plans to maximize compatibility, assess the adequacy of staffing plans at emergency response facilities, identify alternative facilities capable of supporting emergency response, conduct a review to ensure that responders are not assigned collateral duties that would prevent effective emergency response, and implement site-specific Emergency Action Levels (EALs) to provide an anticipatory response to a credible threat. The “Access Authorization Order” required licensees to enhance the access authorization (AA) program in § 73.56 by requiring more restrictive site access controls for personnel, including expanded, expedited, and more thorough employee background checks. The “Security Personnel Training and Qualification Requirements Order” required licensees to take measures to improve tactical and firearms proficiency and physical fitness of the security forces at nuclear power reactor facilities. Finally, the “Revised DBT Order” required all licensees to revise their physical security plans, safeguards contingency plans, and guard training and qualification plans required by 10 CFR §§ 50.34(c), 50.34(d), and 73.55(b)(4)(ii) to provide protection against this revised DBT.

Nuclear power plant licensees revised their security plans, training and qualification plans, and safeguards contingency plans in response to these orders. The NRC completed its review and approval of all of the revised security plans, training and qualification plans, and safeguards contingency plans on October 29, 2004.

1.3 Regulatory Objectives

The NRC’s objectives for the current rulemaking are to establish and update generically applicable security requirements similar to those previously imposed by the Commission orders issued after the terrorist attacks of September 11, 2001. Additionally, the rulemaking adds several new requirements, not derived directly from the Order requirements, requirements developed as a result of insights gained from implementation of the security orders, review of site security plans, implementation of the enhanced baseline inspection program, and NRC evaluation of force-on-force exercises. The rulemaking also updates the regulatory framework in preparation for the licensing of new nuclear power plants. Finally, it resolves three petitions for rulemaking that were considered during the development of the final rule requirements.

2. Identification and Preliminary Analysis of Alternative Approaches

This section presents preliminary analysis of the alternatives that the staff considered to meet the regulatory goals identified in the previous section. (Section 4 presents a more detailed analysis of the final rule option.) The staff considered two alternatives for revising the power reactor security requirements as discussed below.

2.1 Option 1: No Action

Under Option 1, the no-action alternative, NRC would not amend the current regulations regarding power reactor security. Licensees would continue to comply with the Commission's security orders. This option would avoid certain costs that the rule would impose. However, taking no action would not address several "lessons-learned" identified during the time since the initial review and implementation of the orders. Additionally, taking no action would present a problem for the licensing of new reactors that did not receive the orders. The NRC's security regulations would be out of date, and not represent the minimum requirements the Commission deems necessary to ensure the adequate protection of public health and safety and the common defense and security. This would directly conflict with the Commission's licensing obligations set forth in Section 182 of the Atomic Energy Act of 1954, as amended (AEA).

2.2. Option 2: Amend Regulations to Enhance Power Reactor Security

Under Option 2, NRC would conduct a rulemaking to address changes in several sections of 10 CFR part 73 to enhance security operations at power reactors. These changes entail: (1) revising § 73.55, § 73.56, appendix B, appendix C, and (2) adding § 73.58 to introduce "safety/security interface" requirements and § 73.54 (formerly in § 73.55) to introduce cyber security requirements. 10 CFR part 50 would be revised to contain § 50.54(hh) (formerly in appendix C to part 73) which contains requirements regarding licensee procedures for responding to notifications of potential aircraft threats and for developing guidance and strategies to address the loss of large areas of the plant due to explosions or fires from a beyond-design basis event.

A comprehensive rulemaking would provide a means of addressing the identified issues and concerns with respect to part 73. Through a comprehensive revision, the NRC could (1) ensure that all power reactor licensees and applicants would be subject to uniform regulatory requirements in order to consistently implement measures to enhance security and safety at nuclear power plants; (2) revise current requirements to provide licensees and applicants with some implementation flexibility; (3) address adjustments and changes in security plans that licensees have adopted through the development of the revised licensee security plans; and (4) clarify the language of the existing rule. In addition, codification of these security requirements would enable the NRC to require appropriate security measures for new reactor applicants, permitting it to fulfill the NRC's statutory obligations under the AEA.

The NRC has estimated the benefits and costs of this option, as described in Sections 3 and 4 of this regulatory analysis, and has pursued Option 2 for the reasons discussed in Section 5.

3. Evaluation of Benefits and Costs

This section examines the benefits and costs expected to result from this rulemaking, and is presented in two subsections. Section 3.1 identifies attributes that are expected to be affected by the rulemaking. Section 3.2 describes how benefits and costs have been analyzed.

3.1 Identification of Affected Attributes

This section identifies the factors within the public and private sectors that the regulatory alternatives (discussed in Section 2) are expected to affect. These factors are classified as "attributes" using the list of potential attributes provided by NRC in Chapter 5 of its *Regulatory Analysis Technical Evaluation Handbook*.[1] Affected attributes include the following:

- Safeguards and Security Considerations – The actions are intended to establish requirements that will provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public heath and safety.

- Public Health (Accident) – The action will reduce the risk that public health will be affected by radiological releases resulting from radiological sabotage.

- Occupational Health (Accident) – The action will reduce the risk that occupational health will be affected by radiological releases resulting from radiological sabotage.

- Industry Implementation – The action will require licensees to make facility modifications and to revise their Physical Security Plans, Safeguards Contingency Plans, and Training and Qualification Plans, among other implementation activities. Licensees will be required to submit cyber security plans for NRC review and approval.

- Industry Operation – The action will require licensees to conduct additional security activities beyond those currently required. For example, licensees will need to provide additional on-the-job training for security personnel. The action will also provide licensees with flexibility in eliminating or reducing certain activities. For example, vehicles operated inside a site protected area by an individual with unescorted access to the protected area will no longer need a security escort.

- NRC Implementation – Under the action, NRC will develop or revise guidance and inspection procedures and review changes to licensee security plans as a result of the new requirements.

[1] *Regulatory Analysis Technical Evaluation Handbook, Final Report*, NUREG/BR-0184, Office of Nuclear Regulatory Research, January 1997.

- NRC Operation – The action will require the NRC Operations Center to answer calls from licensees when they discover an imminent or actual threat against the facility, and to answer calls regarding suspicious activity and tampering.

- Regulatory Efficiency – The action will result in enhanced regulatory efficiency through regulatory and compliance improvements, including changes associated with sites using mixed-oxide fuel assemblies.

- Off-Site Property – The action will reduce the risk that off-site property will be affected by radiological releases resulting from radiological sabotage.

- On-Site Property – The action will reduce the risk that on-site property will be affected by radiological releases resulting from radiological sabotage.

Attributes that are *not* expected to be affected under any of the rulemaking options include the following: occupational health (routine); public health (routine); environmental considerations; other government; general public; improvements in knowledge; and antitrust considerations.

3.2 Analytical Methodology

This section describes the process used to evaluate benefits and costs associated with the various regulatory options. The benefits of the rule include any desirable changes in affected attributes (e.g., monetary savings, improved safety resulting from new physical protection requirements) while the costs include any undesirable changes in affected attributes (e.g., monetary costs, increased exposures).

The analysis evaluates several attributes on a quantitative basis. (These include industry implementation, industry operation, NRC implementation, and NRC operation.) Quantitative analysis requires a baseline characterization, including factors such as the number of licensees affected, the nature of the activities currently being conducted, and the types of new or modified systems and procedures that licensees will implement, or will no longer implement, as a result of the rule. However, licensees may respond to the rule in different ways depending on their own site-specific characteristics, such as (1) the physical characteristics of their sites, (2) the current contents of their safeguards contingency plans, security plans, and training and qualification plans, (3) the organizational and managerial characteristics of their operations, and (4) their approaches toward meeting new performance-based criteria. It is beyond the scope of this analysis to characterize and analyze individually affected licensees, in large part because the information that would be needed consists of "Safeguards Information" that is protected under § 73.21.[2] Nevertheless, the analysis proceeds quantitatively for these attributes by making generalizing assumptions. Sections 3.2.1–3.2.4 describe the most significant analytical data and assumptions used in the quantitative analysis of these attributes. Additional details regarding the calculations used in the analysis are presented in the appendices to the analysis.

[2] Safeguards Information under 10 CFR 73.21 includes, for example, Security Plans, Safeguard Contingency Plans, physical protection system designs, security procedures, and information relating to safeguards inspections, audits, and evaluations.

The analysis relies primarily on a qualitative (rather than quantitative) evaluation of several of the affected attributes (safeguards and security considerations, public health, occupational health, offsite property, and onsite property) due to the difficulty in quantifying the impact of the current rulemaking.[3] These attributes will be affected by the regulatory options through the associated reduction in the risks of radiological sabotage damage to the reactor core and the spent fuel. Quantification of any of these attributes would require estimation of factors such as (1) the frequency of attempted radiological sabotage, (2) the frequency with which radiological sabotage attempts are (i.e., pre-rule) and will be (i.e., post-rule) successful, and (3) the impacts associated with successful radiological sabotage attempts.

3.2.1 Baseline for Analysis

This regulatory analysis measures the incremental impacts of the final rule relative to a "baseline," which reflects anticipated behavior in the event that the final regulation is not imposed. The baseline used in this analysis assumes full licensee compliance with existing NRC requirements, including current regulations and relevant orders. Section 4.1 presents the estimated incremental costs and savings of the final rule relative to this baseline.

3.2.2 Security Programs and Program Characteristics

The analysis models 65 sites comprising a total of 104 operating power reactors. It assumes that incremental costs and savings accrue to sites independent of the number of reactor facilities located at each site. It also assumes that the manner in which operating reactors comply with current security requirements is substantially similar (except as indicated in appendix A) and that all operating nuclear power reactors are in full compliance with current requirements imposed by NRC's regulations and Commission orders. As a result, the analysis applies the same average cost per activity to each site, even though in reality some sites will incur higher or lower costs. Each operating licensee is assumed to apply for and receive a single 20-year license extension. Based on the extended license expiration dates, the analysis calculates the average remaining operating life across all reactors as 30 years. Therefore, costs and savings are estimated for the 65 reactor sites over a 30 year period, with each year's costs or savings discounted back at a 7-percent and 3-percent discount rate, in accordance with NUREG/BR-0058, Rev. 4, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission." (See Section 4.1 for these results.)

The final rule also would apply to new reactors. Note that although Watts Bar Unit 2 is a "new" reactor, it differs from the other new reactor applications since it is a continuation of a part 50 construction permit and it is specifically required to meet current licensee requirements. NRC has (as of May 2008) received nine applications to build new nuclear power reactors. For the seven new applications that like Watts Bar Unit 2 would co-locate new reactors with currently operating reactors, this analysis assumes that there is no significant additional incremental cost or savings incurred because security program costs are largely a site-based function, rather

[3] The regulatory efficiency attribute also is evaluated qualitatively, by definition. See NRC's *Regulatory Analysis Technical Evaluation Handbook*, Section 5.5.14.

than a reactor-based function. For the two COL applications that would place new reactors at sites that are not co-located with operating reactors, this analysis estimates that one-time and annual impacts will be less than or equal to the corresponding impacts for operating reactors (i.e., because the development of security plans and systems for the new sites will not require that existing plans and systems be analyzed and reworked). Nevertheless, Section 4 does not reflect any additional incremental cost for the non-co-located reactors due to the uncertainty associated with when and if these facilities actually will be licensed and operated.

3.2.3 Data

Information on operating reactors and shutdown dates has been taken from NUREG-1350, Vol. 19, *NRC Information Digest, 2007-2008 Edition.* To the extent practical, quantitative information (e.g., costs and savings) and qualitative information (e.g., the nature and magnitude of safeguards and security impacts) on attributes affected by the rule has been obtained from, or developed in consultation with, NRC staff, commercial vendors, and available Nuclear Energy Institute data. NRC headquarters and regional staffs discussed their understanding of the potential differences between the new requirements and the current security measures in place at existing licensees and have incorporated available, non-safeguards, information into this regulatory analysis. The NRC sought insight from stakeholders on implementing costs and related issues via questions in the proposed rule *Federal Register* notice and integrated this information into the final rule regulatory analysis.

3.2.4 Additional Assumptions

The analysis assumes that any one-time implementation costs are incurred in calendar year 2010. Ongoing costs of operation are also assumed to begin in 2010, and are modeled on an annual cost basis. Where appropriate, the analysis calculates incremental costs and benefits for only a percentage of sites. In these cases, the results presented in Section 4 for the average site will reflect an appropriate proration of the applicable cost or benefit. The detailed incremental cost and savings calculations are presented in Appendices A and B.

4. Results

This section presents the analytical results which are organized into five separate sections:

- Section 4.1 presents findings on the overall benefits and costs of the final rule under the main analysis.
- Section 4.2 considers the findings relative to NRC's backfit rule.
- Section 4.3 considers the findings on a disaggregated basis.
- Section 4.4 addresses the applicability of a safety goal evaluation to the current rulemaking.
- Section 4.5 describes the information that is provide to the Committee to Review Generic Requirements (CRGR) for information only.

4.1 Benefits and Costs

This section summarizes the benefits and costs estimated for the regulatory options. To the extent that the affected attributes could be analyzed quantitatively, the net effect of each option has been calculated and is presented below. However, some values and impacts could be evaluated only on a qualitative basis.

The results of the benefit-cost analysis are summarized in Exhibits 4-1 and 4-2. Relative to the no-action alternative (Option 1), Option 2 would result in a net quantitative impact estimated between $592.84 million and $859.93 million (7-percent and 3-percent discount rate, respectively), with the majority of the costs associated with Option 2 being incurred by industry.

The analysis estimates that Option 2 will result in qualitative benefits in the following attributes: regulatory efficiency, safeguards and security, public health (accident), occupational health (accident), off-site property, and on-site property. Specifically, the benefits will include enhanced regulatory efficiency through regulatory and compliance improvements, including changes in industry's planning efforts and in NRC's review and inspection efforts. In addition, the rule will result in an increased level of assurance that nuclear power plant licensees can defend against the DBT. There also will be a reduced risk that public health, occupational health, off-site property, and on-site property will be affected by radiological releases resulting from attempted sabotage.

Exhibit 4-1

Summary of Benefits/Savings and Costs/Burdens

Net Monetary Savings (or Costs) - Total Present Value	Non-Monetary Benefits/Costs
Option 1: No Action $0	*Qualitative Benefits and Costs:* None.
Option 2: Action **Industry:** ($590 million) using a 7% discount rate ($857 million) using a 3% discount rate **NRC:** ($2.60 million) using a 7% discount rate ($2.60 million) using a 3% discount rate	*Qualitative Benefits:* Safeguards and Security: Increased level of assurance that nuclear power plants are safeguarded from attacks up to, and including the DBT for radiological sabotage. Regulatory Efficiency: Enhanced regulatory efficiency through regulatory and compliance improvements, including changes in industry's planning efforts and in NRC's review and inspection efforts. Public Health (Accident): Reduced risk that public health will be affected by radiological releases resulting from radiological sabotage. Occupational Health (Accident): Reduced risk that occupational health will be affected by radiological releases resulting from radiological sabotage. Off-Site Property: Reduced risk that off-site property will be affected by radiological releases resulting from radiological sabotage. On-Site Property: Reduced risk that on-site property will be affected by radiological releases resulting from radiological sabotage. *Qualitative Costs:* None.

Exhibit 4-2
Industry Savings and Costs by Section

Section	Average per Site		Total - All Sites			
	One-Time Saving (Cost)	Annual Saving (Cost)	One-Time Saving (Cost)	Annual Saving (Cost)	NPV (7 percent)	NPV (3 percent)
Section 73.54						
Cyber Security Plan	($19,200)	-	($1,248,000)	-	($1,248,000)	($1,248,000)
Cyber Security	($1,175,000)	($275,000)	($76,375,000)	($17,875,000)	($295,838,424)	($419,368,626)
Subtotal for Section 73.54	($1,194,200)	($275,000)	($77,623,000)	($17,875,000)	($297,086,424)	($420,616,626)
Section 73.55						
Update Plans and Procedures	($124,000)	-	($8,060,000)	-	($8,060,000)	($8,060,000)
Video Capture	($42,000)	-	($2,730,000)	-	($2,730,000)	($2,730,000)
Training for Escorts	($4,000)	-	($260,000)	-	($260,000)	($260,000)
Two-Way Radios for Escorts	($3,600)	-	($234,000)	-	($234,000)	($234,000)
Escort Communication	($30,000)	-	($1,950,000)	-	($1,950,000)	($1,950,000)
Uninterrupted Power	($75,000)	-	($4,875,000)	-	($4,875,000)	($4,875,000)
No Single Act	($57,000)	-	($3,705,000)	-	($3,705,000)	($3,705,000)
Target Sets	($59,000)	($3,894)	($3,835,000)	($253,110)	($6,942,602)	($8,691,790)
Heightened Security	($8,000)	-	($520,000)	-	($520,000)	($520,000)
Escort of Vehicles	-	$15,000	-	$975,000	$11,970,732	$18,708,743
Subtotal for Section 73.55	($402,600)	$11,106	($26,169,000)	$721,890	($17,305,870)	($12,317,047)
Section 73.56						
Records	-	($56,000)	-	($3,640,000)	($44,690,734)	($69,845,975)
Individuals Subject to Authorization Program	($9,000)	($4,500)	($585,000)	($292,500)	($4,176,220)	($6,197,623)
Increased Sharing of Medical Records	($8,400)	-	($546,000)	-	($546,000)	($546,000)
5-Year Update of Psychological Assessments	($18,038)	($3,158)	($1,172,438)	($205,238)	($3,692,277)	($5,110,628)

Section 73.56 (continued)						
Development of Psychological Test Thresholds	($3,000)	-	($195,000)	-	($195,000)	($195,000)
Administration of Psychological Assessments (Tests and Interviews)	-	($17,050)	-	($1,108,250)	($13,606,732)	($21,265,605)
Subtotal for Section 73.56	*($38,438)*	*($80,708)*	*($2,498,438)*	*($5,245,988)*	*($66,906,962)*	*($103,160,830)*
Section 73.58						
Safety/Security Interface	($116,500)	($40,000)	($7,572,500)	($2,600,000)	($39,494,453)	($57,462,482)
Subtotal for Section 73.58	*($116,500)*	*($40,000)*	*($7,572,500)*	*($2,600,000)*	*($39,494,453)*	*($57,462,482)*
Section 73, Appendix B						
Physical/Medical Examinations for Security Personnel	($10,000)	($2,500)	($650,000)	($162,500)	($2,645,122)	($3,768,124)
On-The-Job Training	($6,000)	($7,000)	($390,000)	($455,000)	($5,976,342)	($9,120,747)
Qualification of Security Instructors	($6,000)	($1,000)	($390,000)	($65,000)	($1,188,049)	($1,637,250)
Armorer Certification	($6,400)	($9,504)	($416,000)	($617,760)	($8,000,656)	($12,269,860)
Physical Requirements for Security Organization Personnel	-	($4,000)	-	($260,000)	($3,192,195)	($4,988,998)
Drill Exercise	-	($186,000)	-	($12,090,000)	($148,437,079)	($231,988,416)
Subtotal for Section 73, Appendix B	*($28,400)*	*($210,004)*	*($1,846,000)*	*($13,650,260)*	*($169,439,443)*	*($263,773,394)*
Section 73, Appendix C						
None.						
Subtotal for Appendix 73, Appendix C	-	-	-	-	-	-
Total	**($1,780,138)**	**($594,606)**	**($115,708,938)**	**($38,649,358)**	**($590,233,152)**	**($857,330,379)**

Results in 2008 dollars.

The new requirements in the rule are expected to result in specific qualitative benefits listed below:

- The NRC issued orders after September 11, 2001, that required power reactor licensees to implement interim compensatory measures to enhance cyber security at their sites. These security measures required an assessment sufficient to provide protection against the cyber threats at the time of the orders. Subsequently, the NRC amended the final DBT requirements in § 73.1(a) to contain cyber attacks (72 FR 12705, dated March 19, 2007). As licensees implement digital upgrades for many systems at their plants, the potential for adverse consequences from cyber threats will be increased. The final rule requirements will maintain and clarify the intent of the security orders and put into place requirements that are to ensure compliance with the revised DBT requirements, by establishing the requirement for a cyber security program to protect systems that, if compromised, can adversely impact safety, security or emergency preparedness.

- The final rule requires licensees to update their physical security, training and qualification, and safeguards contingency plans within 180 days of the effective date of the final rule. Licensees must revise the plans required by § 73.55(c) of the final rule, along with corresponding revisions to all relevant procedures. The new requirement ensures that licensees maintain up-to-date plans and procedures so that they are able to take appropriate actions in preparation for and response to a security-related incident.

- Current requirements at 10 CFR 73.55(h)6) address the use of closed circuit television systems for monitoring of the protected area perimeter, but do not explicitly require them. Nonetheless, the NRC is aware that all licensees have adopted the use of video surveillance in their site security plans, and many licensees have adopted advanced video surveillance technology to provide real-time and play-back/recorded video images to help security officials determine the cause of an alarm annunciation. The final rule, in paragraph 73.55(e), requires the monitoring of isolation zones with assessment equipment that can provide real-time and play-back/recorded video images. Advanced video technology will provide greater assurance that a licensee can assess the cause of an alarm annunciation and initiate a timely response capable of defending the facility against hostile acts up to and including the design basis threat.

- The final rule, paragraph 73.55(g)(8), will ensure that escorts are trained and knowledgeable of their duties while accompanying visitors. This requirement will reduce the risk of a security incident initiated by a visitor because escorts will be better informed regarding visitor's authorized activities.

- The final rule, paragraph 73.55(g)(8)(ii), requires that licensees ensure that individuals assigned to visitor escort duties are provided a means of timely communication with security personnel in a manner that ensures the ability to summon assistance when needed. The new requirement improves security at sites by ensuring that escorts have the ability to call for assistance before that capability can be removed as the result of a security-related incident.

- The final rule, paragraph 73.55(g)(8)(iii), states that each individual assigned to vehicle escort duties must be capable of maintaining continuous communication with security personnel to ensure the ability to summon assistance when needed. This new requirement ensures that escorts have the ability to maintain a direct line of communication with security personnel (e.g., by radio).

- Current regulatory requirements at 10 CFR 73.55(e) and (f) require that both CAS and SAS have equivalent alarm annunciation and communication capabilities, but do not explicitly require equivalent assessment, monitoring, observation, and surveillance capabilities. Further, the current requirement of § 73.55(e)(1) states "All alarms required pursuant to this part must annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station not necessarily onsite, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm." The Commission orders added enhanced detection and assessment capabilities, but did not require equivalent capabilities for both CAS and SAS. The security plans approved by the Commission on October 29, 2004, varied, due to the performance-based nature of the requirements, with respect to how the individual licensees implemented these requirements, but all sites were required to provide CAS and SAS with functionally equivalent capabilities to support the implementation of the site protective strategy.

  Section 73.55(i)(4)(iii) of the final rule states that applicants for an operating license under the provisions of part 50, or holders of a combined license under the provisions of part 52, shall construct, locate, protect, and equip both the central and secondary alarm stations to the standards for the central alarm station in § 73.55, and that both alarm stations shall be equal and redundant, such that all functions needed to satisfy the requirements of this section can be performed in both alarm stations. However, this requirement does not apply to current licensees or new reactors that use a design certified before the final rule takes effect. For new reactors covered by COL applications that already have been submitted to the NRC, therefore, the NRC staff believes this requirement will not be applicable.

- Paragraph 73.55(i)(4)(i) of the final rule requires protecting the alarm stations such that a single act does not disable the key functions will provide an enhanced level of assurance that a licensee can maintain detection, assessment and communications capabilities required to protect the facility against the design basis threat of radiological sabotage.

- Current regulatory requirements at 10 CFR 73.55(e)(1) require back-up power for alarm annunciation and non-portable communication equipment, but do not require uninterruptible back-up power. Although not specifically required, many licensees have installed uninterruptible power supplies to their security systems for added reliability. Uninterruptible back-up power for intrusion assessment and detection equipment at the protected area perimeter, as required now by paragraph 73.55(i)(2)(vii), will provide an enhanced level of assurance that a licensee can maintain capabilities required to defend

the facility against the design basis threat. This new requirement will reduce the risk of losing detection and assessment during a loss of the normal power supply.

- The development of target sets is not a current regulatory requirement. Although the orders did require licensees to maintain target sets, the final rule contains additional target set requirements. The final rule, paragraph 73.55(f), requires licensees to document and maintain the process used to develop and identify target sets, identify and document target set equipment or elements including equipment that is not contained within a protected or vital area, and update target set documentation as needed. Licensees benefit from the new target set requirements because the identification and protection of target sets is a critical component for the development and implementation of the licensee protective strategy.

- Paragraph 73.55(k)(1)) of the final rule requires licensees to establish, maintain and implement a threat warning system which identifies protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. The primary benefit of the heightened security requirement is that licensees will be better prepared to respond to security-related incidents, thus increasing public health and safety.

- Vehicles operated inside a protected area (PA) by individuals with unescorted PA or vital area access no longer need a security escort, as was required by paragraph 73.55(d)(4). Under the final rule, paragraph 73.55(g)(3), only vehicles operated by individuals without unescorted access will need to be escorted, and only vehicles transporting hazardous materials need be escorted by an armed member of the security organization. Currently all vehicles inside the PA must be escorted by a member of the security organization, producing an unnecessary burden on the physical protection of a facility. This change is made possible by the improvement of the unescorted access authorization programs in § 73.56.

- The final rule, paragraph 73.56(b)(1)(ii), will require licensee access authorization programs to cover individuals whose job duties and responsibilities permit them to access or use digital computer systems that may affect licensees' operational safety and security systems, and emergency response capabilities. Historically, digital computer systems have played a limited role in the operation of nuclear power plants. However, the role of computer systems at nuclear power plants is increasing as licensees take advantage of digital technology to maximize plant productivity. In general, licensees currently exclude from their access authorization programs individuals who may electronically access equipment located in the protected areas of nuclear power, if their duties and responsibilities do not require physical unescorted access to the equipment located within protected or vital areas. However, because these individuals may manage and maintain the networks that connect to equipment located within protected or vital areas, and are responsible for permitting authorized and/or trusted personnel to gain electronic access to equipment and systems, they are often granted greater electronic privileges than the trusted and authorized personnel. With advancements in electronic technology and telecommunications, differences in the potential adverse

impacts of a saboteur's actions through physical access and electronic access are lessening. Thus, the final rule will require those individuals who have authority to access equipment electronically that, if compromised can adversely impact operational safety, security or emergency preparedness of the nuclear power plants, to be determined to be trustworthy and reliable.

- The final regulatory requirements at paragraph 73.56(e) specify that licensees, applicants, and contractors or vendors must develop procedures regarding communications between the licensed psychologist/psychiatrist and other medical personnel. The new requirement enables the licensed psychologist/psychiatrist to report any information, including a medical condition, that could adversely impact the fitness-for-duty, trustworthiness, or reliability of those individuals who have been granted unescorted access authorization status.

- The final rule, paragraph 73.56(e), requires a licensed psychiatrist or psychologist to administer the psychological assessment and it requires the licensed medical professional to develop thresholds for the psychological test. The predetermined thresholds will be applied in interpreting the results of the test to determine whether an individual must be interviewed by a licensed psychiatrist or psychologist. Additionally, paragraph 73.56(i)(1)(v)(B) of the final rule requires licensees to update psychological assessments every five years for those individuals who perform duties that are critical to the safety and security of the nuclear power plant. The new requirement not only provides greater consistency and accuracy of the psychological test, but also provides increased assurance that individuals who perform duties that are critical to the safety and security of the nuclear power plant are able to carry out their specific job functions effectively.

- Paragraph 73.56(o) of the final rule requires licensees to document and retain records relating to an individual's unescorted access authorization status and written agreement of services. The new requirement states that licensees must maintain these records for at least five years after an individual's unescorted access authorization has been removed. The requirement to retain all documentation and records for five years ensures that those individuals involved in legal proceedings related their termination of unescorted access have access to their records during the entire course of the legal proceedings.

- Section 73.58 of the final rule requires licensees to assess and manage potential adverse effects on safety and security when implementing changes to plant configurations, facility conditions or security. Licensees are required to review and update existing procedures to reference the safety/security interface requirements, as well as revise and update the corresponding guidance documents. The final safety/security interface requirements will reduce the risk of adverse safety/security interactions and enhance the communication among nuclear power plant staff.

- The NRC is aware that some licensees permit unarmed security personnel to perform duties similar to armed security personnel, including detection, assessment, vehicle and

personnel escort, and vital area controls. The current requirements for unarmed members of the security organization at 10 CFR part 73, appendix B, paragraph I.B.1.a. state in part that these individuals shall have no physical weaknesses or abnormalities that would affect their performance of assigned duties. However, the current rule does not require unarmed personnel to pass a physical examination to verify that they meet standards for vision, hearing, or some portions of psychological qualifications. Appendix B, VI.B.2(a)(2) of the final rule includes a requirement to assure that unarmed security personnel are physically capable of performing their assigned duties. Additionally, appendix B, paragraph I.A.2. of the current rule specifies a minimum age of 21 years for armed security personnel, but does not specify a minimum age requirement for unarmed security personnel. Appendix B, paragraph VI.B.1(a)(2) of the final rule requires that unarmed members attain the age of 18 years prior to assignment. These additional requirements will assure that personnel performing security functions whether, armed or unarmed, meet appropriate age, vision, hearing and psychological requirements commensurate with their assigned security duties.

- The current rule states at appendix B, paragraph II.D., in part, that each individual is assigned security duties shall, prior to assignment, be trained to perform these tasks and duties, and must demonstrate the required knowledge, skill and ability in accordance with specific standards of each task. Appendix B, paragraph VI.C.2. of the final rule now requires licensees to develop on-the-job training plans and procedures. The on-the-job training program will provide licensees the ability to assess an individual's knowledge, skill, and ability to effectively carry out assigned duties, in a supervised manner within the actual work environment, before assignment to an unsupervised position.

- The current rule and the security orders do not specifically address the qualification or certification of instructors, or other personnel that have assigned duties and responsibilities for implementation of training and qualification programs at power reactor licensees. Appendix B, paragraph IV.E of the final rule includes requirements that personnel who have assigned duties and responsibilities for implementation of training and qualification programs be qualified and/or certified to make determinations of the suitability of security personnel. These requirements will result in more effective training, which subsequently results in a more effective security force.

- Appendix B, paragraph VI.G.3.(a) of the final rule requires licensees to develop a firearms maintenance and accountability program that includes armorer certification. To implement this rule requirement, armorers will need to get training and certification on the weapons used at their facility (this regulatory analysis assumes that each armorer will receive one week of training per weapon every three years). This requirement will increase safety by ensuring that weapons and ammunition are properly maintained, function as designed, and are properly stored and accounted for. Additionally, the armorer certification requirement will provide licensees with the assurance that security personnel have functional equipment to assume their security duties upon assignment.

- The current rule and the security orders do not specifically address the qualification of personnel who have assigned duties and responsibilities for implementing security-

related training and qualification drills and exercises at power reactor licensees. Appendix B, paragraph VI.C.3.(l)(4) of the final rule will include requirements for personnel that function as drill and exercise controllers to ensure these persons are trained and qualified to execute their assigned duties. Drills and exercises are key elements to assuring the preparedness of the security force. Performing drills with qualified personnel provides added assurance that the drills and exercises will provide meaningful results and improve a licensee's ability to implement the protective strategy as described in the site security plans effectively.

4.2 Backfit Analysis

This section presents the NRC's evaluation of changes in the rule in accordance with the Backfit Rule, § 50.109.

The backfit analysis examines the aggregation of the subset of power reactor security requirements that constitute backfitting as defined in 10 CFR 50.109(a)(1). These provisions are identified later in this section. The backfit analysis examines the impacts of the rule relative to the baseline used in the regulatory analysis, which consists of existing requirements stated in 10 CFR part 73 as well as requirements in the recently issued orders. The analysis excludes individual requirements that are not subject to the Backfit Rule or that are not backfitting by definition, which includes requirements that fall into one or more of the following categories:

- Administrative matters. Revisions that make minor administrative changes, such as correction of typographic errors, correction of inconsistencies, relocating requirements from one section to another, and combining existing requirements into a single section.

- Information collection and reporting requirements. Revisions that either amend existing information collection and reporting requirements or impose new information and collection and reporting requirements, which are not considered to be backfits, as set forth in the Committee to Review Generic Requirements (CRGR) charter.

- Clarifications. Revisions that clarify current requirements to assure consistent understanding and implementation of the NRC's original intent for these requirements. These revisions remove the ambiguities that produced regulatory uncertainty without changing the underlying requirements stated in these sections.

- Permissive relaxations/Voluntary alternatives. Revisions that permit, but do not require, relaxations or alternatives to current requirements (i.e., licensees are free to either comply with current requirements or adopt the relaxed requirements/voluntary alternative as a binding requirement).

- Requirements that are similar to the provisions required by the recent Commission orders (Interim Compensatory Measures (ICM), February 25, 2002;

> Access Authorization, January 7, 2003; Revised Design Basis Threat, April 29, 2003, and; Security Personnel Training and Qualification Requirements (Training), April 29, 2003) are not backfitting as defined by 10 CFR 50.109(a)(1), and therefore a backfit analysis is unnecessary for these requirements. Section 50.109(a)(1) defines backfitting as "the modification or addition to systems, structures, components or design of a facility … or the procedures or organization required to design, construct or operate a facility; any of which may result from a new or amended provision in the Commission rules…." This first set of requirements in the final rule contains numerous requirements substantially similar to those previously imposed by the orders identified above. In some cases, more specific detail may have been provided in this final rule for a particular requirement that corresponds with a requirement that had previously been in an order. Nonetheless, the provisions in this first set impose requirements that are substantially similar to those previously imposed to current licensees under the orders, and are consistent with the implementing guidance that has been issued to licensees subsequent to the orders. Therefore, the first set of requirements do not constitute backfits as defined by the rule because they would not result in a modification or addition to any systems, structures, components or design of an affected facility, or the procedures or organization required to design, construct or operate an affected facility. In any event, the Commission has also determined that the requirements represented in this first set are those necessary to ensure that these facilities provide adequate protection to the health and safety of the and are in accord with the common defense and security. Therefore, no backfit analysis has been prepared with respect to these requirements

The NRC then evaluated the aggregated set of requirements constituting backfitting in accordance with § 50.109, and not subject to one of the exceptions stated in paragraph 50.109(a)(4), to determine if the costs of implementing the rule would be justified by a substantial increase in public health and safety or common defense and security. In performing this analysis, the NRC considered the quantitative and qualitative costs and benefits of the rule, as discussed below.

Security Regulatory Requirements that Constitute Backfitting

- The cyber security plan must be approved by the Commission and must establish procedures to comply with cyber security programmatic requirements, such as training and hardware modifications, in accordance with § 73.54.

- Security plans and procedures (excluding the cyber security plan, which is analyzed separately in § 73.54) must be revised to address certain requirements in the final rule, though these plans do not have to be submitted to the NRC for prior approval.

- Assessment capabilities must include specialized video surveillance equipment.

- All personnel assigned escort duty must be properly trained and meet other minimum standards, such as access authorization, communication abilities, knowledge of authorized activities, and description of escort-visitor ratios.

- All individuals assigned to escort personnel must be provided with a means of timely and continuous communication.

- Uninterruptible power supplies to maintain alarm and assessment capabilities are required.

- No single act can cause the loss of key functions in both alarm stations.

- Target set equipment documentation and maintenance must be developed in accordance with the requirement set forth in § 73.55.

- Licensees must establish, maintain, and implement a threat warning system.

- Licensees must implement enhanced access authorization requirements.

- Licensees must develop new procedures to increase communication between the licensed psychologist or psychiatrist and the licensee.

- A licensed psychologist or psychiatrist must administer the psychological assessment, using pre-determined thresholds developed by a medical professional to assess the mental state of the individual receiving the test.

- Licensees must revise existing “change control” procedures to address safety/security interface requirements.

- Licensees must test the vision, hearing, and medical condition of unarmed members of the security organization assigned to "unsupervised" duties involving detection, assessment, and response.

- Licensees must provide additional on-the-job training to security personnel including developing on-the-job training plans and procedures.

- Licensees must ensure that security instructors receive specified training to qualify them to perform their duties.

- Licensees must implement a firearms maintenance and accountability program that includes armorer certification.

- Unarmed security personnel must, on an annual basis, meet physical requirements commensurate with their duties.

- Licensees must conduct drills and exercises in accordance with NRC-approved security plans.

Collectively, the requirements in the rule that qualify as backfitting will result in an estimated net cost of approximately $590.23 million to industry over the next 30 years (present value), assuming a 7-percent discount rate, or approximately $857.33 million assuming a 3-percent discount rate.

For the average site, these backfits will result in an initial one-time cost of approximately $1.78 million, followed by annual costs of about $594,600 per year. For industry as a whole, NRC estimates that the backfits will result in approximately $115.71 million in one-time costs, and about $38.65 million in annual costs.

The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these "annualized" one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

The NRC evaluated the safety benefits afforded by the backfitting resulting from the final power reactor security rule revisions, as documented in Section 4.1 of the regulatory analysis, in qualitative terms. (See Section 3.2 of this document for a discussion of the issues that will be involved in quantifying the benefits of the rule.) NRC also qualitatively determined whether the costs of the backfitting required by this rule will be justified in light of the safety benefits. By contrast, the NRC evaluated backfitting costs and cost reductions in quantitative terms, as documented in appendix A of this regulatory analysis.

In performing this analysis, the NRC considered the nine factors in § 50.109, as follows:

(1) Statement of the specific objectives that the backfit is designed to achieve;

The rulemaking constitutes an integrated regulatory initiative directed at the singular regulatory matter of security requirements at nuclear facilities. The goals of the final rule will be as follows:

- Make generically applicable security requirements similar to those imposed by Commission orders issued after the terrorist attacks of September 11, 2001, based upon experience and insights gained by the Commission during implementation.

- Add several new requirements that resulted from insights from implementation of the security orders, review of site security plans, and implementation of the enhanced baseline inspection program and force-on-force exercises.

- Update the regulatory framework for the licensing of new reactors.

- Impose requirements to assess and manage site activities that can adversely affect safety and security.

(2) General description of the activity that will be required by the licensee or applicant in order to complete the backfit;

In general terms, the final rule will require that all current and future power reactor licensees consistently implement new and existing security measures. These new measures include revisions to existing "change control" procedures to address safety/security interface requirements to avoid adverse safety-security interactions. The backfits include several requirements targeted at enhancing intrusion detection and assessment system technologies in the CAS and SAS. These enhancements include uninterruptible power for detection and assessment equipment. The backfits required in appendix B address physical qualifications and training for security personnel. The final rule extends armed security personnel requirements for vision, hearing, medical, and physical qualifications to unarmed security personnel, commensurate with their duties. In terms of training, the final rule requires on-the-job training for armed and unarmed members of the security organization, qualification of training instructors, and qualification or certification of drill and exercise controllers. The final rule will maintain the intent of the security orders and put in place requirements to meet the revised DBT by establishing the requirement for a cyber security program to protect any systems that if compromised, can adversely impact safety, security or emergency preparedness. Detailed analysis of the activities and procedural changes required by the rule are set forth in appendix A of this regulatory analysis.

(3) Potential change in the risk to the public from the accidental off-site release of radioactive material;

The rulemaking is intended to provide added assurance that the risk of offsite releases as a result of breaches in security at nuclear power plants is acceptably low and consistent with the NRC's Safety Goals. However, the reduction in risk to the public from offsite releases of radioactive materials has not been fully quantified because there is insufficient information and modeling to support such quantification (see Section 3.2).

(4) Potential impact on radiological exposure of facility employees;

The rulemaking will provide added assurance that nuclear industry workers are not subjected to unnecessary radiological or hazardous chemical exposures as the result of a breach in security that causes an accident leading to a release of radiation which workers then are exposed to as the result of mitigative and/or clean-up activities.

(5) Installation and continuing costs associated with the backfit, including the cost of facility downtime or the cost of construction delay;

The backfit analysis for the final power reactor security rule sets forth the NRC's estimate of the initial costs for implementing the major elements of the rule, and the ongoing costs and savings to the licensees. The estimated one-time industry net cost associated with the backfits will be approximately $115.71 million (or approximately $1.73 million for the average program), and the annually recurring cost will be approximately $38.65 million (or approximately $553,600 for the average program). Combining these initial and annual costs, this analysis estimates that the backfits associated with the power reactor security rule will cost industry approximately $590.23 million (present value, assuming a 7-percent discount rate) to $857.33 million (present value, assuming a 3-percent discount rate).

(6) The potential safety impact of changes in plant or operational complexity, including the relationship to final and existing regulatory requirements;

The power reactor security rule will make changes with respect to the design of a nuclear power plant. Specifically, the changes involve the following:

- The CAS and SAS must not be susceptible to both being lost to a single act;
- Advanced video surveillance systems must be installed; and
- The intrusion detection and assessment system must have an uninterrupted power source.

For new reactors:

- Both the CAS and the SAS must maintain functionally-equivalent capabilities.

These design changes do not affect all nuclear power plants because some currently meet these requirements. This rule is not expected to have a significant effect on facility complexity.

The rule will require modifications to training and "change control" procedures. These "costs" in terms of increased complexity in security procedures are detailed in appendix A of this regulatory analysis. The added complexity is not expected to be significant or to substantially impact licensees' operational practices or to result in substantial indirect costs.

(7) The estimated resource burden on the NRC associated with the backfit and the availability of such resources;

The rulemaking will result in a substantial increase in one-time expenditures of agency resources for the NRC to review and approve licensees' cyber security plans, and subsequently inspect implementation of licensee cyber security programs. Additionally, the NRC estimates that in the first year of implementation, it will spend 276 hours to revise implementation guidelines and inspection procedures. These activities will result in a one-time cost of approximately $2.60 million.

The rulemaking will not result in a substantial increase in annual expenditures of agency resources.

(8) The potential impact of differences in facility type, design or age on the relevancy and practicality of the backfit;

The security requirements in part 73 do not directly relate to the facility type, design or age. Although the benefits and costs attributable to the power reactor security rule will vary for a variety of site-specific reasons (e.g., facility layout, geography, choice of protective strategies), the NRC does not believe they will vary based upon the facility type, design or age.

(9) Whether the backfit is interim or final and, if interim, the justification for imposing the backfit on an interim basis.

The backfitting will be final.

The NRC finds that the backfitting contained in the final power reactor security rule, when considered in the aggregate, will constitute a substantial increase in protection to public health and safety and security. For reasons that were discussed in Section 3.2, it is not feasible to quantify the safety benefits of the rule. Nevertheless, NRC believes that the rule is warranted for several qualitative reasons. First, the final rule will provide assurance of licensees' capabilities to protect their sites against the DBT of radiological sabotage defined in § 73.1, in accordance with § 73.55(b). Second, there have been technological advances in intrusion detection systems that maintain an effective protection system and failure to implement these technologies could erode assurance that the physical protection system will perform as intended during a safeguards contingency. Third, the rule will increase the assurance that no single act could remove the functions of both the SAS and CAS. Fourth, the rule will increase licensees' security program effectiveness through procedures such as on-the-job training and increased qualification training. NRC believes that these factors represent a substantial increase in safety and that the rulemaking has merit on the basis of these stated qualitative reasons.

In light of the findings above, the NRC submits that the qualitative safety benefits of the power reactor security rule provisions that qualify as backfitting, considered in the aggregate, will constitute a substantial increase in protection to public health and safety and the common defense and security, and that the costs of this rule will be justified in view of the increase in protection to safety and security provided by the backfitting embodied in the rule.

4.3 Disaggregation

In order to comply with the guidance provided in Section 4.3.2 ("Criteria for the Treatment of Individual Requirements") of the Regulatory Analysis Guidelines, the NRC conducted a screening review to ensure that the aggregate analysis does not mask the inclusion of individual rule provisions that are not cost-beneficial when considered individually and not necessary to meet the goals of the rulemaking. Consistent with the Regulatory Guidelines, the NRC evaluated, on a disaggregated basis, each of the 25 new regulatory provisions expected to result in incremental costs or savings. Based on this screening review, the NRC staff has determined that each of the requirements is needed and is cost-justified relative to its qualitative benefits.

4.4 Safety Goal Evaluation

Safety goal evaluations are applicable only to regulatory initiatives considered to be generic safety enhancement backfits subject to the substantial additional protection standard at § 50.109(a)(3).[4] Some aspects of the rule may qualify as generic safety enhancements because they may affect the likelihood of core damage or spent fuel damage, which generally are the focus of a quantitative safety goal evaluation. However, the magnitude of this change is not readily quantifiable due to uncertainties discussed in Section 3.2 above. A more dominant effect of the rule is to reduce the probability of other types of damage associated with a wide array of acts of sabotage, although this effect is equally difficult to quantify. Because the change in safety associated with the rulemaking cannot be quantified, the regulatory changes cannot be compared to NRC's safety goals.

4.5 CRGR Results

This section addresses regulatory analysis information requirements for rulemaking actions or staff positions subject to review by the Committee to Review Generic Requirements (CRGR). All information that will be provided to the CRGR for information is presented in this regulatory analysis, or in the Federal Register notice for the final power reactor security rule. As a reference aid, Exhibit 4-4 provides a cross-reference between the relevant information and its location in this document or the Federal Register notice. Note that the rulemaking process was recently revised by Commission SRM dated October 25, 2007, and as a result, this information is provided to the CRGR for information only, not for review and approval.

[4] A safety goal evaluation is not needed, therefore, for new requirements falling within the backfit exceptions at 10 CFR 50.109(a)(4)(i)-(iii).

Exhibit 4-4
Specific CRGR Regulatory Analysis Information Requirements

CRGR Charter Citation	Information Item to be Included in a Regulatory Analysis Prepared for CRGR Review (information only)	Where Item is Discussed
IV.B(1)	Generic requirement or staff position as it is to be sent out to licensees. When the objective or intended result of a generic requirement or staff position can be achieved by setting a readily quantifiable standard that has an unambiguous relationship to a readily measurable quantity and is enforceable, the requirements should specify the objective or result to be attained rather than prescribing how the objective or result is to be attained.	Rule text in Federal Register Notice
IV.B(iii)	The sponsoring office's position on whether the action will increase requirements or staff positions, implement existing requirements or staff positions, or relax or reduce existing requirements or staff positions.	Regulatory Analysis, Section 4.1
IV.B(iv)	The method of implementation.	Regulatory Analysis, Section 6
IV.B(vi)	Identification of the category of power reactors or nuclear materials facilities/activities to which the generic requirement or staff position will apply.	Regulatory Analysis, Section 3.2.2 and 4.2
IV.B(vii) IV.B(viii)	If the action involves a power reactor backfit and the exceptions at 10 CFR 50.109(a)(4) are not applicable, the items required at 10 CFR 50.109(c) and the required rationale at 10 CFR 50.109(a)(3) are to be included.	Regulatory Analysis, Section 4.2
IV.B(x)	For relaxations or decreases in current requirements or staff positions, a rationale is to be included for the determination that (a) the public health and safety and the common defense and security will be adequately protected if the reduction in requirements or positions were implemented, and (b) the cost savings attributed to the action will be substantial enough to justify taking the action.	Federal Register Notice for the rule
IV.B(xii)	Preparation of an assessment of how the action relates to the Commission's Safety Goal Policy Statement.	Regulatory Analysis, Section 4.4

5. Decision Rationale

5.1 Regulatory Analysis

Relative to the “no-action” alternative, the final rule will result in a net cost estimated as approximately $592.84 million (total present value over a 30-year period), assuming a 7-percent discount rate, or approximately $859.93 million assuming a 3-percent discount rate. All of this cost will accrue to industry, except for approximately $2.6 million that will accrue to the NRC. The rule will result in one-time industry costs of approximately $115.71 million. This is equivalent to approximately $1.78 million for the average reactor site. The final rule language will generate annual industry costs of about $38.65 million ($594,600 per site). Offsetting this net cost, the NRC believes that the rule will result in substantial non-quantified benefits related to safety and security, as well as enhanced regulatory efficiency and effectiveness. The analysis presents these benefits in Section 4.1 of this document. Based on the NRC's assessment of the costs and benefits of the propose rule on licensee facilities, the agency has concluded that the final rule provisions will be justified.

The final rule will result in an annual impact to the economy of approximately $47.36 million (using a 7 percent discount rate, annualizing the one-time costs over 30 years, and adding these “annualized” one-time costs to the annual costs) or $44.38 (using a 3 percent discount rate). This final rule is therefore not a major rule as defined by the Congressional Review Act.

5.2 Backfit Analysis

The NRC conducted a backfit analysis of the power reactor security rule relative to the backfitting requirements in 10 CFR 50.109. Certain requirements of the final rule do constitute backfitting because they will result in the modification of or addition to systems, structures, components or design of a nuclear power plant, or the procedures or organization required to design, construct, or operate a facility. The measures constituting backfitting, in general, include establishing cyber security programs to protect computer systems; updating security plans and relevant procedures; enhancing intrusion detection and assessment system technologies in the CAS and SAS; developing and implementing safety/security interface procedures to avoid adverse safety/security interactions; extending armed security personnel requirements for vision, hearing, medical, and physical qualifications to unarmed security personnel; conducting on-the-job training for new armed and unarmed members of the security organization and drill exercises. These new measures meet the definition of a backfit because such efforts will be new and will be the result of additional or modified provisions in the NRC's current rules.

The NRC believes that the backfitting required by this rule is cost-justified for several qualitative reasons. First, the rule will provide additional assurance of licensees’ capability to protect the power reactor sites against assaults up to and including the DBT of radiological sabotage. Second, the rule will require uninterruptible power supplies and extension of the “no single act” criterion to key alarm station functions. In this regard the rule will also result in the deployment of certain technological advances in intrusion detection systems that are enhancements during

a safeguards contingency. Third, in recognition of advancing digital technology, the rule will maintain the intent of the security orders and put in place requirements for meeting the radiological sabotage DBT by establishing the requirement for a cyber security program to protect any systems that could, if compromised, adversely impact safety, security or emergency preparedness. Fourth, the rule will increase licensees' security program effectiveness through additional training and qualification measures, including safety/security interface, on-the-job training and armorer certification. NRC concludes that these factors represent a substantial increase in safety and that the rulemaking has merit on the basis of these stated qualitative reasons.

6. Implementation

This section identifies how and when the rule will be implemented, the required NRC actions to ensure implementation, and the impact on NRC resources.

6.1 Schedule

The final rulemaking will become effective on 30 days following publication in the Federal Register. It is expected that the final rule will be published in early, to mid, 2009. The final rule requires that within 180 days, each currently operating reactor licensee must evaluate, on a site-specific basis, what security plan changes are needed to comply with the amended requirements of the final rule. Those changes must be incorporated into their security plans, as necessary. In doing so, licensees are expected to follow the appropriate change processes described currently in § 50.54(p), § 50.90 or § 73.5. Section 73.54 requires licensees to submit a cyber security plan within 180 days of the effective date of the rule for NRC review and approval.

6.2 Impacts on Other Requirements

As discussed in Section 4.1, affected licensees will experience most of the impact of the revisions to 10 CFR part 73. The rulemaking will result in a substantial increase in one-time expenditures of agency resources for the NRC to review and approve licensees' cyber security plans, as well as subsequent inspections of licensee cyber security programs. Additionally, the NRC estimates that in the first year of implementation, it will spend 276 hours to revise implementation guidelines and inspection procedures. These activities will result in a one-time cost of approximately $2.60 million. However, the NRC does not expect that the rulemaking subsequently will result in a substantial increase in annual expenditures of agency resources.