NUREG-1885

Report to Congress on the Security Inspection Program for Commercial Power Reactor and Category I Fuel Cycle Facilities: Results and Status Update

Annual Report for Calendar Year 2006

Manuscript Completed: August 2007
Date Published: September 2007

Division of Security Operations
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This report fulfills the requirements of Chapter 14, Section 170D of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended by the Energy Policy Act of 2005, which states, "not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year." This is the second annual report which covers calendar year 2006. In addition to information on the security response evaluation program (force-on-force exercises), the NRC is providing additional information regarding the overall security performance of the commercial nuclear power industry and selected fuel cycle facilities to keep Congress and the public informed of the NRC's efforts to protect the nation's electric power infrastructure and special nuclear material against terrorist attacks.

Paperwork Reduction Act Statement

This NUREG does not contain information collection requirements and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

Page

ABSTRACT iii

EXECUTIVE SUMMARY vii

ABBREVIATIONS ix

1. INTRODUCTION 1

2. REACTOR SECURITY OVERSIGHT PROCESS 3
   2.1 Overview 3
   2.2 Significance Determination Process 5

3. FORCE-ON-FORCE INSPECTION PROGRAM 7
   3.1 Overview 7
   3.2 Program Activities in 2006 7
   3.3 Results of Inspections 8
   3.4 Discussion of Corrective Actions 10
   3.5 Future Planned Activities 10

4. BASELINE SECURITY INSPECTION PROGRAM 13
   4.1 Overview 13
   4.2 Results of Inspections 13

5. OVERALL REACTOR SECURITY ASSESSMENT 15
   5.1 Overview 15
   5.2 Performance Indicators 15
   5.3 Security Cornerstone Action Matrix 15

6. CAT I FACILITY SECURITY INSPECTION PROGRAM 17
   6.1 Overview 17
   6.2 Results of Inspections 17

7. STAKEHOLDER COMMUNICATIONS 19
   7.1 Communications with Public and Industry 19
   7.2 Communications with Local, State, and Federal Agencies 20

Appendices

Appendix A: 2005 Annual Report to Congress on the Security Inspection Program A-1

Figures

Figure 1: Cornerstones of the Reactor Oversight Process 3
Figure 2: Inspectable Areas of the Safeguards Cornerstone 4

Tables

Table 1: CY 2006 FOF Inspection Program Summary 9
Table 2: Cumulative FOF Inspection Program Results 9
Table 3: CY 2006 Security Inspection Program Results (Without FOF) 14
Table 4: Summary of Security Action Matrix 16

EXECUTIVE SUMMARY

This report fulfills the requirements of Chapter 14, Section 170D of the Atomic Energy Act of 1954 (42 U.S.C. 2201 et seq.), as amended by the Energy Policy Act of 2005, which states, "not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year." This is the second annual report which covers calendar year (CY) 2006. In addition to information on the security response evaluation program (force-on-force inspections), the NRC is providing additional information regarding the overall security performance of the commercial nuclear power industry and selected fuel cycle facilities to keep Congress and the public informed of the NRC's efforts to protect the nation's electric power infrastructure and special nuclear material (SNM) against terrorist attacks.

The NRC is committed to protecting public health and safety, promoting the common defense and security, and protecting the environment. Conducting the security inspection program, which includes performance-based force-on-force (FOF) inspections, is one of a number of regulatory oversight activities the NRC performs to ensure the secure, safe use and management of radioactive materials by the commercial nuclear industry. In support of these activities, the NRC employs relevant intelligence information and vulnerability analyses to determine realistic and practical security requirements and mitigative strategies. Further, a risk-informed, graded approach is used to establish appropriate regulatory controls, enhance NRC inspection efforts, assess the significance of issues, and to influence timely and effective corrective action by licensees of commercial nuclear power plants for identified deficiencies. These practices utilize interagency cooperation in the development of an integrated approach to the security of nuclear facilities and contribute to NRC's comprehensive evaluation of licensee security performance.

This report describes the results of the NRC's security inspection program, including the nuclear reactor security baseline inspection program, security of Category I (CAT I) fuel cycle facilities, and exercises conducted as part of FOF inspections. The reporting period included herein is January 1, 2006, through December 31, 2006.

During CY 2006, the NRC conducted 298 security inspections at nuclear power plants (of which 21 were FOF inspections). These inspections identified 73 findings of which 67 were of very low security significance and 6 were of low to moderate security significance. The results of the security inspections conducted at CAT I fuel cycle facilities are discussed in the classified version of this report.

PAGE INTENTIONALLY LEFT BLANK

ABBREVIATIONS

ASM	additional security measure
BWXT	BWX Technologies
CAF	composite adversary force
CAT I	Category I
CY	Calendar Year
DBT	design basis threat
DOD	Department of Defense
DOE	Department of Energy
EPA	Energy Policy Act
FOF	force-on-force
HEU	highly-enriched uranium
IDS	intrusion detection system
MC&A	material control and accounting
MILES	Multiple Integrated Laser Engagement System
NCV	non-cited violation
NFS	Nuclear Fuel Services
NPP	nuclear power plant
NR	Office of Naval Reactors
NRC	U.S. Nuclear Regulatory Commission
OCA	owner controlled area
PA	protected area
PI	performance indicator
PPSDP	Physical Protection Significance Determination Process
ROP	reactor oversight process
SDP	significance determination process
SL	severity level
SNM	special nuclear material
SSNM	strategic special nuclear material
URI	unresolved item

PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

The Energy Policy Act of 2005 amended Chapter 14, Section 170D of the Atomic Energy Act to require, in part, that "not less often than once each year, the Commission shall submit to the Committee on Environment and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives a report, in classified form and unclassified form, that describes the results of each security response evaluation conducted and any relevant corrective action taken by a licensee during the previous year." This report fulfills the requirement for an unclassified report.

Last year, the U.S. Nuclear Regulatory Commission (NRC) provided to Congress the first annual report on the results of the NRC's security inspection program. In addition to outlining the results of the overall security inspection program for Calendar Year (CY) 2005, the report described the evolution of the NRC's security inspection program from the days preceding September 11, 2001, to the current program. This report for CY 2006 conveys the results of inspections for the reporting period, but will not describe the evolution of the program. For that background information, the 2005 report is included as Appendix A as a reference.

This report provides an overview of the NRC's security inspection program and force-on-force (FOF) program and summaries of the results of those inspections. NRC's communications and outreach activities with the public and other stakeholders (including other federal agencies) will also be described. Unless otherwise noted, this report does not include security activities or initiatives of any class of licensee other than power reactors or Category I fuel cycle facilities. Category I fuel cycle facilities are those which use or possess formula quantities of strategic special nuclear material (SSNM). SSNM is defined in 10 CFR as uranium-235 (contained in uranium enriched to 20 percent or more in the U235 isotope), uranium-233, or plutonium.

PAGE INTENTIONALLY LEFT BLANK

2. REACTOR SECURITY OVERSIGHT PROCESS

2.1 Overview

The NRC continues to implement the Reactor Oversight Process (ROP) which is the agency's program for ensuring plant and radiological safety, security, and emergency preparedness at operating nuclear power plants. The basic principles and philosophy of the ROP are to ensure that a defined, repeatable, and objective process is applied to identify findings, determine their significance, and document results in accordance with ROP program guidance. Program instructions and inspection procedures help provide assurance that licensee actions and regulatory response are commensurate with the safety or security significance of the particular event, deficiency, or weakness. Within each ROP cornerstone (see Figure 1), NRC residents and regional specialist inspectors conduct inspections using detailed inspection procedures whose results, in the aggregate, contribute to an overall assessment of licensee performance.

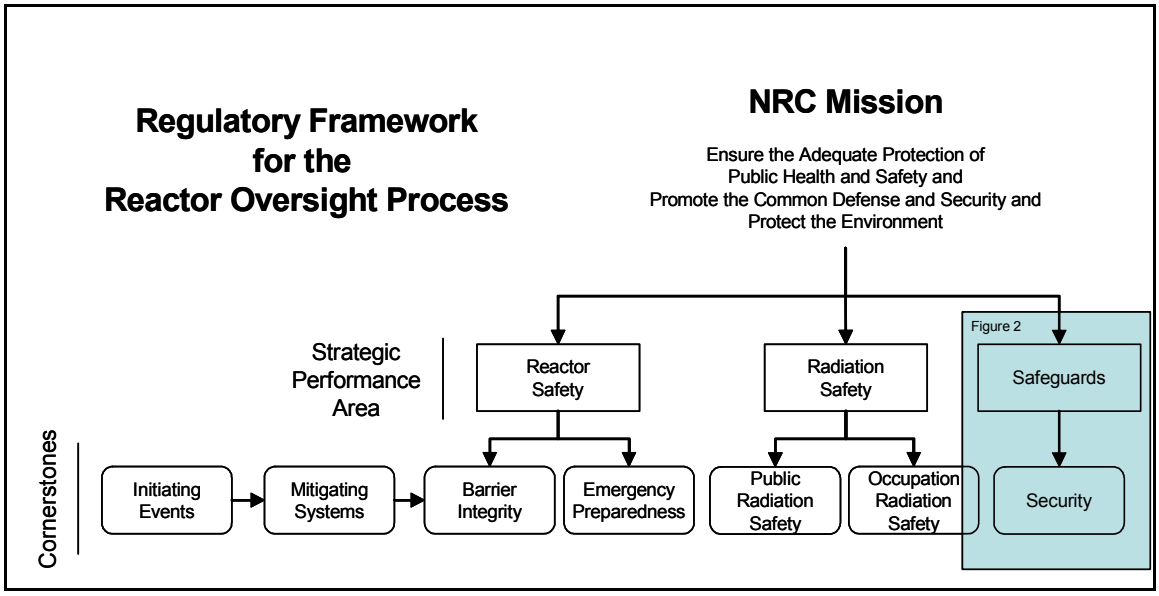


Figure 1: Cornerstones of the Reactor Oversight Process

As part of post 9/11 actions, the NRC issued a number of Orders requiring licensees to strengthen security programs in a number of areas. Based on those Orders, the NRC significantly enhanced its baseline security inspection program for commercial nuclear power plants (NPP). This inspection effort resides within the "Security Cornerstone" of the agency's ROP. The Security Cornerstone focuses on five key licensee performance attributes: access authorization; access control; physical protection; material control and accounting (MC&A); and response to contingency events. Through the results obtained from all oversight activities, including baseline security inspections and performance indicators (PI), the NRC determines whether licensees comply with requirements and can provide assurance of adequate protection against the design basis threat (DBT) for radiological sabotage.

The Security Cornerstone has four objectives: (1) to obtain information providing objective evidence that the security and safeguards at NRC-licensed NPPs are maintained in a manner that contributes to public health and safety and promotes the common defense and security; (2) to determine that licensees have established measures to deter, detect, and protect against the DBT of radiological sabotage as required by regulations and other Commission mandates such as orders; (3) to determine the causes of declining performance in the physical protection arena before such performance reaches a level that may result in a degradation to reactor safety or undue risk to public health and safety; and (4) to identify those significant issues that may have generic or cross-cutting applicability. These objectives help ensure the secure use and management of radioactive materials.

Licensees currently report data on three performance indicators in security: (1) Protected Area Equipment; (2) Personnel Screening Program; and (3) Fitness-for-Duty/Personnel Screening Program. The data reported by the licensees are compared to an established set of thresholds to determine their significance, which is represented by the colors green, white, yellow, and red (in order of increasing severity). The PIs measure aspects of the licensees' security programs that are not specifically inspected by the NRC's baseline inspection program.

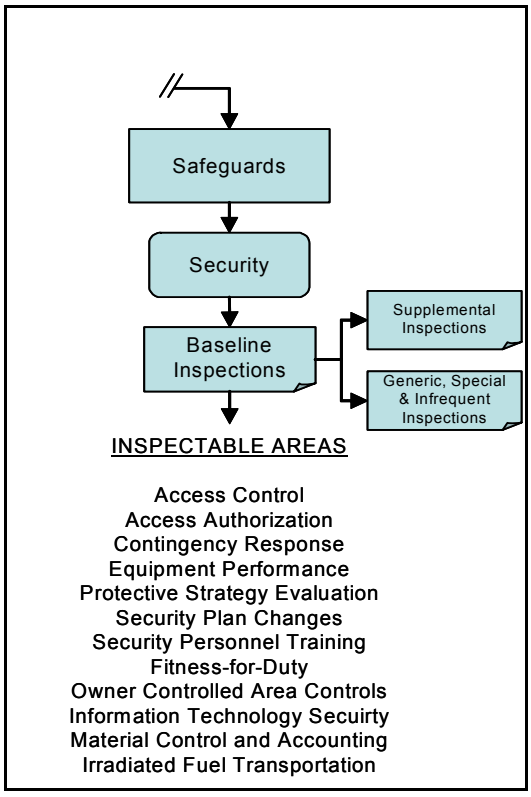


Figure 2: Inspectable Areas of the Safeguards Cornerstone

The baseline inspection program requires 12 “inspectable areas” to be reviewed periodically at each facility (see Figure 2). One of the inspectable areas, contingency response, is assessed through the conduct of FOF inspections, described in detail in the next section. In addition, MC&A inspections are conducted to ensure that licensees take adequate measures to control the risk of loss, theft, or diversion of SNM.

Where performance issues have been identified at a particular licensee, supplemental inspections may be conducted to further investigate a particular deficiency or weakness. In certain situations, the NRC may conduct a generic, special, or infrequent inspection. Such an inspection is not part of the baseline or supplemental inspection program and would only be conducted after a review and assessment of a particular security or safeguards event or condition. These types of inspections include, but are not limited to: resolution of employee concerns, security matters requiring particular focus, licensee plans for coping with strikes, and inspection of international safeguards. During this reporting period, there were three special inspections at NPPs. These special inspections covered topics such as: blast vulnerabilities, inadequate searches of packages and material, and improper compensatory measures.

2.2 Significance Determination Process

The Significance Determination Process (SDP) for NPPs uses risk insights, where appropriate, to help NRC inspectors and staff determine the security significance of inspection findings. Security-related findings are evaluated using the baseline Physical Protection Significance Determination Process (PPSDP). These findings include both programmatic and process deficiencies. The PPSDP provides the security significance of any security program deficiency. If it is unclear whether or not an observation is a finding, it will be documented in the inspection report as an unresolved item (URI) until clarifying information can be gathered. A URI is an issue about which more information is required to determine if it is acceptable, if it is a finding, or if it constitutes a deviation or violation. Such a matter may require additional information from the licensee or may require additional guidance or clarification/interpretation of the existing guidance. Certain violations that cannot be evaluated by the PPSDP are assigned a severity level based on the NRC’s Enforcement Policy.

FOF findings are evaluated using the FOF SDP. The significance of findings associated with FOF adversary actions are dependent on how far into the plant the mock adversary force progresses, their impact on critical equipment (referred to as a target set), and a determination of whether or not these actions could have had an adverse impact on public health and safety. Other security-related findings identified during FOF activities are also evaluated using the baseline PPSDP. These findings may include programmatic and process deficiencies that are not directly related to a FOF inspection outcome, but are identified during the FOF exercise. In situations where the NRC cannot clearly determine the outcome of an exercise, the exercise will be considered indeterminate and an additional exercise scheduled, if appropriate.

PAGE INTENTIONALLY LEFT BLANK

3. FORCE-ON-FORCE INSPECTION PROGRAM

3.1 Overview

A full FOF inspection, spanning several days, includes both table-top drills and exercises that simulate combat between a mock commando-type adversary force and the licensee security force. At a nuclear power plant, the adversary force may attempt to reach and damage key safety systems and components that protect the reactor's core or the spent fuel pool, potentially causing a radioactive release to the environment. At other facilities, the adversary force may attempt theft or diversion of SNM. The licensee's security force, in turn, seeks to prevent the adversaries from causing such a release or theft. In addition to significant participation of plant operators and NRC personnel, these exercises may include observers from an array of Federal, state, and local law enforcement agencies and emergency planning officials.

In conducting FOF inspections, NRC notifies the licensee in advance for safety and logistical purposes. This notification provides adequate planning time for licensee coordination of two sets of security officers - one for maintaining actual plant security and the other for participating in the exercise. In addition, arrangements must be made by the licensee for a group of individuals who will control and monitor each exercise. A key goal of the NRC is to balance safety (both personnel and operational) while maintaining actual plant security during an exercise that is as realistic as possible.

In preparation for an FOF exercise, information from table-top drills, which probe for potential deficiencies in the licensee's protective strategy, other baseline security inspections, and security plan reviews are factored into a number of commando-style attack scenarios. The objective of the site's responders is to prevent the attackers from destroying or damaging (simulated in an FOF exercise) critical equipment (target sets) the theft or diversion of SNM. Any potential deficiencies in the protective strategy identified during FOF exercises are promptly reviewed and corrected before NRC inspectors leave the licensee's site.[1]

3.2 Program Activities in 2006

In 2006, the FOF inspection program focused on effectively evaluating licensee protective strategies while maintaining regulatory stability and consistency in the evaluation process. The staff continued to work with the nuclear industry to improve the standard of training and qualification for exercise controllers. In 2007, the staff endorsed industry's revised controller guidance document for the remainder of the current inspection cycle which ends in December 2007. The NRC remains committed to working with the industry to improve the realism and effectiveness of the FOF inspection program and will continue to pursue methods to improve certain exercise simulations and the controller responses to those simulations.

The composite adversary force (CAF) used for NPP inspections continued to meet expectations for a credible, well-trained and consistent mock adversary force. In order to meet security clearance requirements, the staff enlisted a composite adversary team from the Office of Naval

[1] See "Protecting Our Nation," and Office of Public Affairs "Backgrounder" on Force-on-Force. http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/

Reactors (NR) to conduct FOF exercises at CAT I fuel cycle facilities instead of the CAF, who are only cleared for safeguards information. The NR adversary team all had Department of Energy (DOE) Q clearances.

In improving its own processes, the NRC took part in benchmarking efforts with other agencies that conduct similar security performance assessments. NRC staff observed FOF exercises conducted by the DOE and the Department of Defense (DOD). DOE and DOD representatives observed NRC FOF exercises as well. These interagency observations were in an effort to share best practices among agencies.

3.3 Results of Inspections

Between January 1, 2006, and December 31, 2006, FOF inspections were conducted at 21 commercial NPPs. During the conduct of FOF inspections, two findings related to other areas of the security baseline program were identified. These findings included: failure to provide adequate detection at a barrier; and failure to adequately evaluate the effectiveness of a change to the Physical Security Plan. As of the end of 2006, FOF inspections have been conducted at 45 out of a total of 66 sites[2] (including both commercial power reactor and CAT I fuel cycle facilities). Table 1 below summarizes the 21 inspections conducted at NPPs in CY 2006. Details on the results of the inspections conducted at the CAT I fuel cycle facilities are discussed in the classified version of this report.

Violations and non-cited violations (NCV) of NRC requirements are categorized by significance, and are given corresponding color or severity level (SL) codes. For inspection findings evaluated with the SDP, violations are assigned colors, as follows: green (very low security significance); white (low to moderate security significance); yellow (substantial security significance); and red (high security significance). White, yellow and red findings are considered greater than green.

Violations that are not evaluated through the SDP are categorized in terms of four levels of severity to show their relative importance or significance. SL I has been assigned to violations that are the most significant and SL IV violations are the least significant. SL I and II violations are of very significant regulatory concern. In general, violations that are included in these severity categories involve actual or high potential consequences on public health and safety. SL III violations are cause for significant regulatory concern. SL IV violations are less serious but are of more than minor concern. Violations at SL IV involve noncompliance with NRC requirements that are not considered significant based on risk.

[2]NOTE: For the purposes of the security inspection program, Salem and Hope Creek are counted as one site, as they share a common security program, bringing the total number of reactor sites to 64.

Table 1: CY 2006 FOF Inspection Program Summary at NPPs	
21	Total number of inspections conducted.
2	Total number of inspection findings.
1	Total number of Green findings.
0	Total number of greater than Green findings.
1	Total number of SL IV violations.
0	Total number of greater than SL IV violations.

Table 2 below summarizes the cumulative results of the FOF inspections conducted at NPPs since the current cycle began in November 2004. During a FOF inspection, three FOF exercises are scheduled. If an exercise is canceled due to severe weather or other reasons, NRC management may consider less than three exercises only when a licensee has successfully demonstrated an effective strategy in at least two exercises, with no significant issues identified. If those conditions are not met, the team may have to expand the schedule or schedule a subsequent visit.

Of the total number of exercises conducted, four exercises were inconclusive and deemed indeterminate. An indeterminate exercise is one where the NRC inspectors are prevented from effectively gathering sufficient information to evaluate the licensee's protective strategy or to form a cogent conclusion. These exercises were indeterminate due to: excessive safety or administrative holds; insufficient exercise control; or extreme malfunctions of exercise simulation systems. Another four exercises were canceled because of potential safety concerns associated with dangerous weather conditions or a plant transient.

Table 2: Cumulative FOF Inspection Program Results at NPPs	
44	Total number of inspections conducted.
43	Total number of inspection sites.
128	Total number of exercises conducted.
0	Total number of times a complete target set damaged or destroyed.
5	Total number of inspection findings.
4	Total number of Green findings.
0	Total number of greater than Green findings.
1	Total number of SL IV violations.
0	Total number of greater than SL IV violations.

3.4 Discussion of Corrective Actions

If inspectors identify deficiencies during the conduct of FOF inspection activities that indicate a licensee cannot demonstrate the ability to protect against the applicable DBT or does not meet other regulatory requirements, that licensee must take immediate corrective actions. NRC inspectors review any proposed compensatory measures and/or corrective actions, and once determined acceptable, must verify that those actions have been completed by the licensee before leaving the site. As appropriate, the licensee must also plan for long term corrective actions, with oversight from the NRC.

In many cases, though not required by regulation, licensees implement corrective actions in response to lessons learned from FOF inspections, even after demonstrating that their protective strategy can effectively protect against the DBT. Those corrective actions typically fall into one of three categories: procedural or policy changes; physical security and/or technology improvements and upgrades; and personnel or security force enhancements. In CY 2006, FOF inspectors have observed corrective actions taken in each of these categories.

As an example of a procedural or policy change, one licensee kept keys for a security response vehicle in an unprotected area. During an FOF exercise, the CAF team acquired those keys and used the vehicle to facilitate its simulated attack. Although the licensee was not in violation of NRC requirements and demonstrated an effective protective strategy, the site's security management recognized the potential vulnerability, and made procedural changes to enhance its protective strategy based on the FOF exercise.

Licensees will also commonly make improvements to or add physical security structures and technologies based on lessons learned from FOF exercises. For example, if a licensee determines that the adversary team did not encounter enough delay throughout the simulated attack, extra delay barriers, such as fences, or locks on doors or gates, may be added. As another example, if a licensee determines that earlier detection and assessment is necessary (even after demonstrating an effective protective strategy in FOF exercises), they may choose to add sensors, cameras and/or lighting to the owner controlled area (the area of the facility beyond the boundary of the protected perimeter).

Finally, licensees may commit to additional security personnel as a result of lessons learned from FOF exercises. Inspectors have observed situations where licensees determined that additional margin was necessary to ensure that adversaries would be interdicted before completing their mission.

3.5 Future Planned Activities

In CY 2007, 23 FOF inspections are scheduled to complete the current inspection cycle. Two of the twenty-three are follow-up inspections to test improvements resulting from previous FOF inspections. Although significant enhancements have been made, the NRC will continue to seek additional methods to improve realism in FOF exercises during the third year of this 3-year inspection cycle.

In the CY 2005 annual report, the NRC reported that an inspection had been postponed at a facility because of the impact of Hurricane Katrina and that the inspection would be rescheduled

in 2006. The facility was, in fact, rescheduled for late 2006, but had to be rescheduled later in the cycle to make that time slot available for another facility that needed immediate assessment because of performance concerns in the area of security. The FOF inspection for the former facility was completed in May 2007. The results of that inspection will be captured in the CY 2007 report to Congress.

In addition to completing the inspection cycle, in CY 2007, NRC staff will integrate beyond-DBT training exercises into the FOF program, with voluntary participation from the industry. For the licensees that volunteer, a beyond-DBT training exercise will be substituted for the third evaluated exercise provided that the protective strategy was conclusively demonstrated with high assurance in the first two evaluated exercises, with no significant issues identified during those exercises. These training exercises will offer the opportunity for licensee security forces to face an increased threat, and for the NRC to observe how the licensees' protective strategies adjust to that increased threat.

PAGE INTENTIONALLY LEFT BLANK

4. BASELINE SECURITY INSPECTION PROGRAM

4.1 Overview

The baseline security inspection program is a primary component of the Security Cornerstone of the ROP that the NRC uses to ensure plant and radiological safety, security, and emergency preparedness at operating NPPs. It is important to note that FOF inspections are just one piece of the NRC's overall security oversight process. In addition to FOF inspections, the baseline security inspection program includes: Access Authorization; Access Controls; Security Plan Changes; Equipment Performance, Testing and Maintenance; Protective Strategy and Evaluation; Security Training; the Fitness for Duty Program; Owner Controlled Area Controls; Information Technology Security; Material Control and Accounting; and Physical Protection of Shipments of spent nuclear fuel. These inspections are conducted by specialist inspectors from both regional offices and headquarters, as well as resident inspectors.

4.2 Results of Inspections

Table 3 summarizes the overall results of the security baseline inspection program of NPPs, including MC&A inspection results, but excluding FOF inspection results (which were discussed in Section 3). This information provides a summary overview of licensee performance within the Security Cornerstone.

For the purpose of this report, an inspection is considered complete after: (1) the inspection report is issued with no findings; or, (2) any findings have been dispositioned or any applicable enforcement action has been taken.

Violations and non-cited violations (NCV) of NRC requirements are categorized by significance, and are given corresponding color or severity level (SL) codes. For inspection findings evaluated with the SDP, violations are assigned colors, as follows: green (very low security significance); white (low to moderate security significance); yellow (substantial security significance); and red (high security significance). White, yellow and red findings are considered greater than green.

Violations that are not evaluated through the SDP are categorized in terms of four levels of severity to show their relative importance or significance. SL I has been assigned to violations that are the most significant and SL IV violations are the least significant. SL I and II violations are of very significant regulatory concern. In general, violations that are included in these severity categories involve actual or high potential consequences on public health and safety. SL III violations are cause for significant regulatory concern. SL IV violations are less serious but are of more than minor concern. Violations at SL IV involve noncompliance with NRC requirements that are not considered significant based on risk.

Table 3: CY 2006 Security Inspection Program Results (Without FOF)	
277	Total number of inspections conducted.
71	Total number of inspection findings.
60	Total number of Green findings.
2	Total number of greater than Green findings.
5	Total number of SL IV violations.
4	Total number of greater than SL IV violations.
3	Total number of special inspections conducted.

5. OVERALL REACTOR SECURITY ASSESSMENT

5.1 Overview

The previous two sections described the results of FOF inspections and the rest of the baseline security inspection program. The security assessment process collects the information from those inspections and other performance indicators provided by NPP licensees to enable the NRC to arrive at objective conclusions about a licensee's performance in security. Based on this assessment information, the NRC determines the appropriate level of agency response.

5.2 Performance Indicators

Licensees voluntarily report data on three performance indicators in security: (1) Protected Area Equipment; (2) Personnel Screening Program; and (3) Fitness-for-Duty/Personnel Screening Program. The data reported by the licensees are compared to an established set of thresholds to determine their significance, which is represented by the colors green, white, yellow, and red (in order of increasing severity). The PIs measure aspects of the licensees' security programs that are not specifically inspected by the NRC's baseline inspection program.

As of the end of CY 2006, all licensees reported that each security performance indicator was categorized as green.

5.3 Security Cornerstone Action Matrix

Similar to the ROP action matrix, the security cornerstone has five response columns: Licensee Response; Regulatory Response; Degraded Cornerstone; Repetitive Degraded Cornerstone; and Unacceptable Performance. Table 4 summarizes the security cornerstone action matrix.

Most licensees fall into the Licensee Response column, which indicates that all assessment inputs (PIs and inspection findings) were green and the cornerstone objectives were fully met. Licensees that fall into the Regulatory Response column have assessment inputs that resulted in no more than one white input, and the cornerstone objective was met with minimal reduction in security performance. In CY 2006, three sites fell into this column.

The Degraded Cornerstone column describes licensees that had multiple white inputs or one yellow input, with the cornerstone objective met with moderate degradation in security performance. If a licensee falls into the Repetitive Degraded Cornerstone column, they have received multiple yellow inputs or one red input, while meeting the cornerstone objective with longstanding issues or significant degradation in security performance. The most significant column in the security action matrix is the Unacceptable Performance column. Licensees in this column have overall unacceptable performance and margin for security. In CY 2006, no licensees fell into the Degraded Cornerstone, Repetitive Degraded Cornerstone, or Unacceptable Performance categories.

Table 4: Summary of Security Action Matrix[3]	
Number of Sites	**Response Band**
61	Licensee Response
3	Regulatory Response
0	Degraded Cornerstone
0	Repetitive Degraded Cornerstone
0	Unacceptable Performance

[3]NOTE: For the purposes of security inspection program, Salem and Hope Creek are counted as one site, as they share a common security program, bringing the total number of reactor sites to 64.

6. CAT I FACILITY SECURITY INSPECTION PROGRAM

6.1 Overview

The NRC implements regulatory oversight of safeguards and security programs of two CAT I fuel cycle facilities. BWX Technologies (BWXT), located in Lynchburg, Virginia, and Nuclear Fuel Services (NFS), located in Erwin, Tennessee, manufacture fuel for government reactors. They also downblend highly-enriched uranium (HEU) into low-enriched uranium (LEU) for use in commercial reactors. Each CAT I facility stores and processes strategic special nuclear material (SSNM), which must be reliably protected against unauthorized access, and theft and diversion. The facilities have significantly enhanced their security posture since September 11, 2001. NFS is currently implementing a major program of additional security upgrades.

The primary objectives of the CAT I security oversight program are to ensure that the fuel cycle facilities are operating safely and securely in accordance with regulatory requirements and Commission Orders; detect indications of declining safeguards performance; investigate specific safeguards events and weaknesses; and identify generic security issues. NRC headquarters and regional specialist inspectors conduct inspections using detailed inspection procedures whose results, in the aggregate, contribute to an overall assessment of licensee performance.

The NRC CAT I core inspection program is implemented by inspectors based at NRC offices in Atlanta, Georgia and Rockville, Maryland. Similar to the reactor baseline inspection program, it is applied to identify findings, determine their significance, document results, and assess licensee's corrective actions. The core inspection program requires three physical security areas ("inspection procedure suites") to be reviewed annually at each CAT I facility. These include HEU access control, HEU alarms and barriers, and other security topics such as security force training and contingency response. The core inspection program also requires two MC&A inspections annually and a transportation security inspection once every three years. NRC regional inspectors also review the U.S. Department of Energy's (DOE) audits of licensees' programs to protect classified material and information.

The core inspection program is complemented by the FOF inspection program, which is implemented by the NRC Headquarters. In addition, NRC resident inspectors, assigned to each CAT I facility, provide an onsite NRC presence for direct observation and verification of licensee's ongoing activities. Through the results obtained from all oversight efforts, the NRC determines whether licensees comply with regulatory requirements and can provide assurance of adequate protection against the DBT for theft and diversion of CAT I SSNM.

Similar to the ROP, plant-specific supplemental or reactive inspections may be conducted to further investigate a particular deficiency or weakness. Such an inspection is not part of the core inspection program and would only be conducted after a review and assessment of a particular security or safeguards event or condition.

6.2 Results of Inspections

The results of CAT I security inspections are included in the classified version of this report.

PAGE INTENTIONALLY LEFT BLANK

7. STAKEHOLDER COMMUNICATIONS

7.1 Communications with Public and Industry

As part of an effort to improve openness to the public, in 2006 the Commission reviewed several options that would make some security oversight information available to the public. The Commission decided to have the cover letters to security-related inspection reports made available in the public domain. However, the information contained in the letters would have to be such that the letters do not identify actual or potential vulnerabilities at the inspected plant. The cover letters for security-related inspection reports issued after May 8, 2006, are now being released to the public.

The restrictions placed on releasing security-related information to the public after September 11, 2001, also impacted the NRC's ability to share information with allegers who brought security-related concerns to the NRC. The restrictions have made it difficult for the staff to assure allegers that their concerns have been addressed, and a number of allegers have expressed dissatisfaction with the NRC's limited response. Some, in an effort to obtain a satisfactory response, have chosen to pursue their concerns publicly by engaging elected officials and public interest groups and by disseminating their concerns via public websites or media outlets. In some instances these actions have necessitated that the staff respond in a public manner to the allegers' concerns. While the allegers were receptive to the feedback provided, at this time, the staff does not consider a public response to be the most advisable primary means of addressing security-related concerns. The Commission has approved a three-tiered approach to responding to security allegers based on the severity of the concern raised and normal availability of the information to the alleger (i.e., the alleger is a member of a licensee's security force).[4]

As an additional effort to improve public awareness and understanding, the NRC held annual public meetings specifically on nuclear security issues in August 2004, September 2005, and September 2006. Additionally, security topics are presented at the NRC's Regulatory Information Conference held each spring in Rockville, Maryland.

NRC also communicates with the industry to disseminate key lessons learned and generic issues. NRC analyzes findings and observations from the security inspection program to determine if a potentially generic issue may exist across the industry. When applicable, NRC staff supplements periodic security meetings held with the industry and develops generic communications or advisories as a means of effective communication. In CY 2006, the NRC issued 9 security advisories covering a variety of topics. After each FOF inspection, NRC staff gathers lessons learned in a variety of categories. Those lessons learned are disseminated to the industry through the Nuclear Security Working Group (NSWG), a consortium of security representatives from NRC-licensed facilities, with the combined goal of safe and realistic performance evaluations.

---

[4]For more information, see SECY 07-0032, "Recommended Staff Actions Regarding Correspondence with Allegers Involving Security-Related Concerns," dated February 12, 2007. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2007/

7.2 Communications with Local, State, and Federal Agencies

In most NRC FOF inspections, representatives from local law enforcement agencies attend planning activities and observe the exercise to improve understanding of the licensee's response and coordination of integrated response activities. Other representatives from State emergency management agencies, State governments, the Government Accountability Office, and Congress have also observed FOF inspections.

The NRC continues to support the U.S. Department of Homeland Security/Homeland Security Council (DHS/HSC) initiative to enhance integrated response planning for power reactor facilities. The staff is continuing to work with DHS/HSC, the Federal Bureau of Investigation (FBI) and others to develop plans to address recommended actions. In addition, the staff has coordinated with other Federal agencies and State and local security partners in completing the development of Emergency Action Levels for all imminent threats[5].

[5]For more information, see NRC Regulatory Issue Summary 2006-12, "Endorsement of Nuclear Energy Institute Guidance 'Enhancement to Emergency Preparedness Programs for Hostile Action'", published on July 19, 2006.
http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2006/

APPENDIX A

PAGE INTENTIONALLY LEFT BLANK

ANNUAL STATUS REPORT ON THE RESULTS OF THE SECURITY INSPECTION PROGRAM CONDUCTED BY THE UNITED STATES NUCLEAR REGULATORY COMMISSION

CALENDAR YEAR 2005

TABLE OF CONTENTS

I Executive Summary A-2

II Background A-3
Prior to September 11, 2001 . . . . . A-3
Response to September 11, 2001 . . . . . A-3

III Baseline Inspection Program A-4

IV Significance Determination Process A-7

V CY 2005 Baseline Security Inspection Results A-8

VI FOF Inspection A-8
Evolution of FOF Inspections A-8
Qualification of FOF Inspectors A-10
Exercise Simulation Systems A-10
Composite Adversary Force A-11
Inspection Procedure 71130.03 Revision A-12
Improved Controller Training and Qualification A-12
Beyond the DBT and Technical Approaches to Beyond DBT A-12
Indeterminate Exercise A-13

VII FOF Regulatory Program Activities A-13

VIII FOF 2006 Planned Activities A-14

IX Disposition of Findings A-14

X Communications A-15

XI Interagency Support A-15

XII Reference List A-16

XIII Acronym List A-17

I Executive Summary

The Energy Policy Act of 2005, H.R. 6, Section 651(e), directed the U.S. Nuclear Regulatory Commission (NRC) to submit an annual report in classified and unclassified form to the Committee on Environmental and Public Works of the Senate and the Committee on Energy and Commerce of the House of Representatives, that describes the results of each of the security response evaluations (i.e., force-on-force exercises) conducted by NRC and any relevant corrective action taken by a licensee. This is the first annual report covering calender year (CY) 2005. The NRC is also providing additional information regarding the overall security performance of the commercial nuclear power industry to keep the Congress and the public informed of the NRC's efforts to help protect the Nation's electric power infrastructure against terrorist attacks.

The NRC is committed to protecting public health and safety, promoting the common defense and security, and protecting the environment. Conducting our security inspection program, which includes force-on-force (FOF) exercises, is one of a number of regulatory oversight activities the NRC performs to ensure the secure use and management of radioactive materials by the commercial nuclear power industry. In support of these activities, the NRC employs relevant intelligence information and vulnerability analyses to determine realistic and practical security requirements and mitigative strategies. Further, a risk-informed, graded approach is used to establish appropriate regulatory controls, enhance NRC inspection efforts, assess the significance of issues, and to influence timely and effective corrective action by licensees of commercial nuclear power plants for identified deficiencies. These practices utilize interagency cooperation in the development of an integrated approach to the security of nuclear facilities and contribute to NRC's comprehensive evaluation of licensee security performance.

During CY 2005, the NRC-conducted security inspections, including FOF exercises at NRC-licensed commercial nuclear power plants (NPP) based on risk insights, security assessments, and logistical considerations. FOF exercises at NRC-licensed Category I (CAT I) fuel cycle facilities were commenced in early CY 2006 and will be described in subsequent annual reports.

This report describes the evolution of the NRC’s security inspection program, including the security baseline inspection program for CY 2005 and details for the FOF program from pre-September 11, 2001, to the present highlighting enhancements to the program. The reporting period included herein is October 29, 2004, through December 31, 2005.

During the reporting period, the NRC conducted 134 inspections (of which 23 were FOF exercises). These inspections identified 107 findings of which 99 findings were of very low security significance and 5 findings were of low to moderate security significance.

II Background

Prior to September 11

Before the terrorist attacks on September 11, 2001, the NRC conducted security inspections at all NPP facilities to ensure compliance with NRC regulations. These included FOF exercises at each commercial NPP approximately once every 8 years. According to NRC regulations, NPP licensees conducted their own FOF exercises on an annual basis, which the NRC observed. However, in the wake of the terrorist attacks, the Commission temporarily suspended the FOF exercises at NPP facilities. The Commission's primary concern was that conducting such exercises could have distracted the licensees' security forces and the NRC staff during a time when licensees needed to focus on implementing the NRC's highest level of alert, as well as numerous security upgrades.[6] Although FOF inspections were temporarily suspended, NRC continued to conduct the baseline security inspection program including its practice to periodically inspect licensees through the use of NRC security specialist inspectors and on-site resident inspectors who maintain daily vigilance over matters of nuclear safety, security, and emergency preparedness, as well as other regulatory activities.

Response to September 11 - Summary of Security Enhancements

In response to the September 11, 2001 terrorist attacks, the NRC immediately advised nuclear power plants to go to the highest level of security in accordance with the system in place at the time. In the weeks and months following September 11, 2001, the NRC focused its efforts on enhancing security at the facilities it regulates. The terrorist attacks reaffirmed the need for collective vigilance, enhanced security and safeguards, and improved emergency preparedness and incident response capabilities throughout the Nation's electrical infrastructure. As a result, the NRC conducted a thorough review of the agency's security and safeguards programs and made enhancements, in part to strengthen its requirements for NRC-licensees and to improve coordination to defend against a more challenging adversarial threat.

On February 25, 2002, the NRC issued Orders to NPP licensees requiring that they increase their defensive capabilities in the post-9/11 threat environment. These enhancements to security included increased security patrols, augmented security forces, additional security posts, increased standoff distances for vehicles, improved coordination with law enforcement and intelligence communities, and strengthened safety-related mitigation procedures and strategies.

On January 7, 2003, the NRC issued another Order requiring further enhancements to access controls for the NPPs. On April 29, 2003, the NRC issued three additional Orders requiring security enhancements in the areas of: 1) a supplemented design basis threat (DBT) for radiological sabotage, 2) enhanced training on tactical and firearms proficiency and physical fitness, and, 3) fitness-for-duty, including security force personnel work-hour limitations. These Orders required all licensees to continue to meet all previous security requirements.

[1] "Protecting Our Nation" (See referenced list in Section XII.)

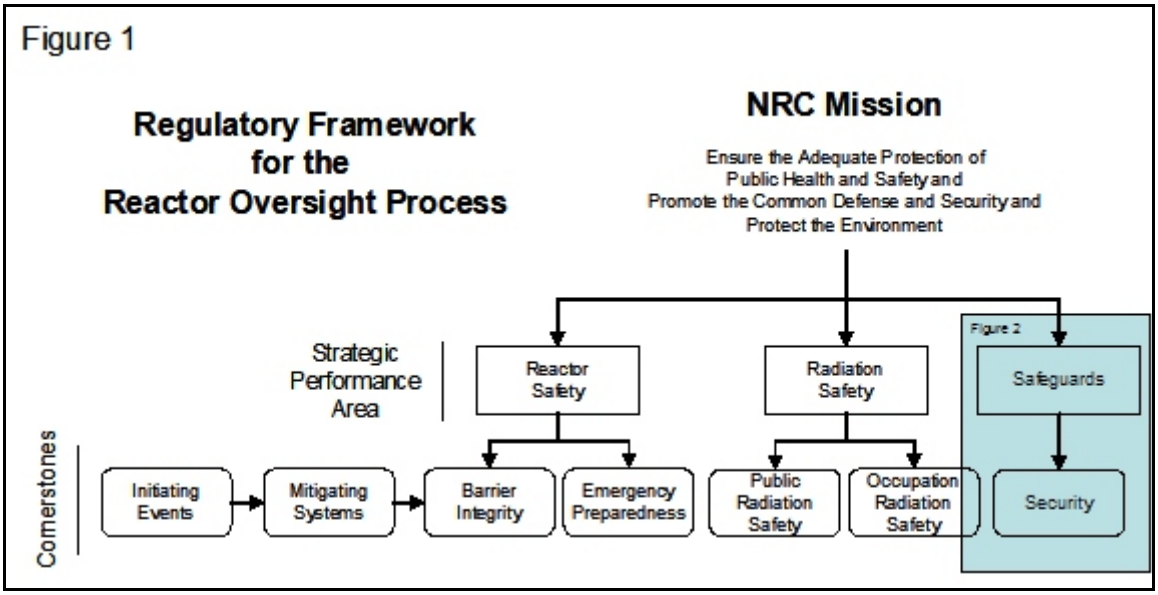
The DBT is a set of adversary characteristics established by the Commission as the basis for the design of the licensee's security systems. In establishing the DBT, the Commission considers intelligence information, protective measures that may be employed (including potential unintended consequences), and availability of such measures to private security forces, to determine the adversary characteristics that are reasonable to expect a private force to protect against.

The April 2003 Orders required all NPP licensees to submit revised security plans to the NRC for review and approval by April 29, 2004, and that the plans be implemented by October 29, 2004. All licensees met this requirement.[7] These measures and others are periodically evaluated by the NRC through its baseline security inspection program, which includes the conduct of FOF inspections. For other NRC licensees, NRC issued similar orders enhancing security-related requirements and measures to protect the public health and safety, to promote the common defense and security, and to protect the environment.

III Baseline Inspection Program

The NRC continues to implement the Reactor Oversight Process (ROP) which is the agency's program for ensuring plant and radiological safety, security, and emergency preparedness at all operating nuclear power plants. The basic principles and philosophy of the ROP are to ensure that a defined, repeatable, and objective process is applied to identify findings, determine their significance, and document results in accordance with ROP program guidance. Program instructions and inspection procedures help provide assurance that licensee actions and regulatory response are commensurate with the safety or security significance of the

Figure 1



[2] Letter from Chairman Diaz to Department of Homeland Security, Secretary Tom Ridge, dated September 8, 2004.

particular event, deficiency, or weakness. Within each ROP cornerstone (see Figure 1), NRC headquarters and regional specialist inspectors conduct inspections using detailed inspection procedures whose results, in the aggregate, contribute to an overall assessment of licensee performance.

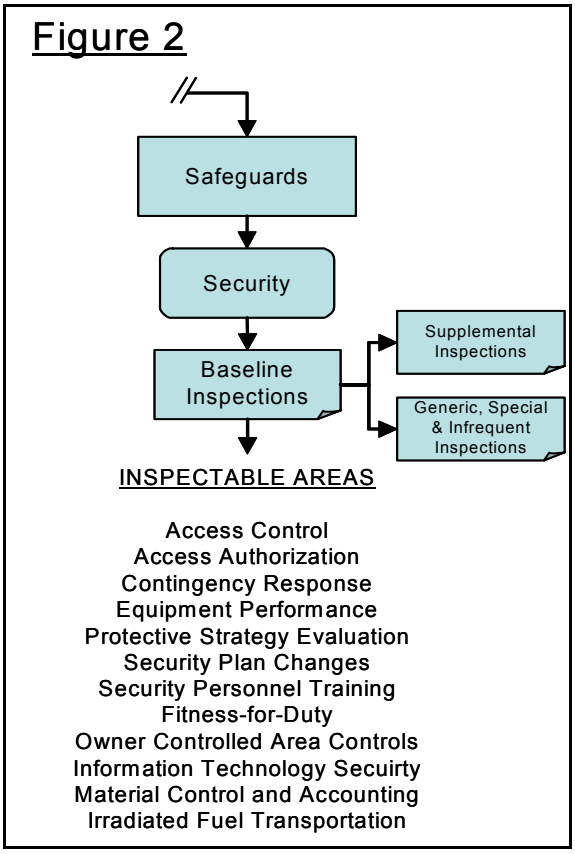
The NRC significantly enhanced its baseline security inspection program for commercial nuclear power plants since September 11, 2001. This inspection effort resides within the "Security Cornerstone" of the agency's ROP. The Security Cornerstone focuses on five key licensee performance attributes: access authorization; access control; physical protection; material control and accounting (MC&A); and response to contingency events. Through the results obtained from all oversight activities, including but not limited to baseline security inspections, the NRC determines whether licensees comply with requirements and can provide high assurance of adequate protection against the DBT for radiological sabotage.

NRC oversight of licensee security capability has increased significantly since the terrorist attacks of September 11, 2001. In 2000, approximately 40 staff-weeks of direct inspection effort were spent on security inspections (excluding FOF exercises) for nuclear power reactors. By 2003, this inspection effort had increased to 205 staff weeks. This effort focused on licensee implementation of compensatory measures to address the post-9/11 threat environment. These compensatory measures were required by the Commission's February 25, 2002, Order. In late 2003, the staff developed the revised baseline inspection program for reactor security, taking into consideration the enhanced requirements and elevated threat environment. The staff began implementation of the revised baseline inspection program in March 2004. These inspections focused on those elements of the program that had been fully implemented under the previous Orders, such as access authorization and security force work hour limits. The NRC also implemented a Management Review Panel to ensure that inspection findings and potential violations are treated in a consistent and appropriate manner. During CY 2005, the inspection effort focused on verifying licensee implementation of the remaining Commission's Orders. The staff expended approximately 400 staff-weeks of direct inspection effort in 2005. Implementation of all elements of the baseline security inspection program commenced in January 2006.

In a related matter, following the terrorist acts of September 11, 2001, the NRC determined that there was a potential that security-related information routinely made public through the NRC web-site and the NRC's public reading rooms could aid potential adversaries seeking to cause radiological sabotage or theft or diversion of radioactive materials. Therefore, the NRC revised its information dissemination policy to ensure that security-related information is not provided to a possible adversary. This policy specifically applied to information related to licensee security and safeguards performance, including generic or nation-wide performance information. As a result, the public is provided limited information on regulatory decisions or actions involving security inspection, assessment, or enforcement. In keeping with the NRC strategic goal of openness in our regulatory process, the Commission reassessed this policy on May 1, 2006, and is making certain results of its security inspection program for commercial NPPs available to the public.

As discussed, the security inspection program for commercial NPPs resides within the Security Cornerstone. The cornerstone has four objectives: (1) to obtain information providing objective evidence that the security and safeguards at NRC-licensed NPPs are maintained in a manner that contributes to public health and safety and promotes the common defense and security;

(2) to determine that licensees have established measures to deter, detect, and protect against the DBT for radiological sabotage as required by regulations and other Commission mandates such as Orders; (3) to determine the causes of declining performance in the physical protection arena before such performance reaches a level that may result in a degradation to reactor safety or undue risk to public health and safety; and (4) to identify those significant issues that



may have generic or cross-cutting applicability. These objectives help ensure the secure use and management of radioactive materials. The baseline inspection program requires 12 "inspectable areas" to be reviewed periodically at each power reactor facility (see Figure 2). In addition, MC&A inspections are conducted to ensure that licensees take adequate measures to control the risk of loss, theft, or diversion of SNM.

Where performance issues have been identified at a particular licensee, supplemental inspections may be conducted to further investigate a particular deficiency or weakness. In certain situations, the NRC Regional Administrator may authorize the conduct of a generic, special, or infrequent inspection. Such an inspection is not part of the baseline or supplemental inspection program and would only be conducted after a review and assessment of a particular security or safeguards event or condition. These types of inspections include, but are not limited to: resolution of employee concerns, security matters requiring particular focus, licensee plans for coping with strikes, and inspection of international safeguards. During the reporting

period, a special inspection was conducted at a NPP to review performance issues with the intrusion detection system.

The NRC is currently evaluating the efficacy of the Physical Security Performance Indicators (PIs) to determine if revisions are warranted to enhance their function as leading indicators, or if a different program would serve the need more efficiently. The PIs are a means of obtaining information related to the performance of certain key attributes in each of the cornerstone areas.

Regulatory response to identified security-related deficiencies is in accordance with an action matrix based on the security significance of the inspection finding. Both the significance of the finding and the actions required are implemented through NRC procedures that ensure such assessments are predictable, repeatable, and commensurate with the event, deficiency, or performance weakness.

IV Significance Determination Process (SDP)

The SDP uses risk insights, where appropriate, to help NRC inspectors and staff determine the security significance of inspection findings. Security-related findings are evaluated using the baseline Physical Protection Significance Determination Process (PPSDP). These findings include both programmatic and process deficiencies. The PPSDP provides the security significance of any security program deficiency. Unresolved items (URI) are discussed within the inspection team, and documented in the inspection report. A URI is an issue about which more information is required to determine if it is acceptable, if it is a finding, or if it constitutes a deviation or violation. Such a matter may require additional information from the licensee or may require additional guidance or clarification/interpretation of the existing guidance.

In July 2004, the staff issued and began piloting a separate Significance Determination Process (SDP) for FOF inspections. The staff completed the FOF SDP pilot in December 2004. In addition to the pilot SDP, the staff applied NRC Inspection Manual Chapter 0609, “Significance Determination” guidance to ensure an objective and common framework was utilized. As lessons learned are compiled throughout the inspection process, the SDP may be reevaluated and revised.

The significance of findings associated with FOF adversary actions are dependent on how far into the plant the mock adversaries force progresses, their impact on critical equipment (referred to as a target set), and a determination of whether or not these actions had an adverse impact on the public.

Force-on-force findings are evaluated using the FOF SDP. Other security-related findings identified during FOF activities are also evaluated using the baseline PPSDP. These findings may include programmatic and process deficiencies that are not directly related to a FOF inspection outcome, but are identified during the FOF exercise. All URIs are discussed within the inspection team, and documented in the inspection report. In situations where the NRC cannot clearly determine the outcome of an exercise, the exercise may be considered indeterminate and any identified process or programmatic deficiencies would be processed through the baseline PPSDP.

V CY 2005 Baseline Security Inspection Program Results

Table 1 summarizes the overall results of the security inspection program excluding FOF inspection results. This information provides a summary overview of licensee performance within the Security Cornerstone.

Violations and non-cited violations (NCV) are categorized by significance, and are given corresponding color or severity level (SL) codes, as follows: green or SL IV (very low security significance); white or SL III (low to moderate security significance); yellow or SL II (substantial security significance); and red or SL I (high security significance). White, yellow and red findings are considered greater than green. Any finding that is greater than green proceeds in the normal enforcement process.

Table 1, CY 2005 Baseline Security Inspection Program Results without FOF Inspections

CY 2005 Baseline Security Inspection Program Results	
111	Total number of inspections conducted across the industry.
104	Total number of inspection findings across the industry.
85	Total number of Green findings.
3	Total number of greater than Green findings.
14	Total number of SL IV violations.
2	Total number of greater than SL IV violations.
6	Total number of special inspections conducted.
0	Total number of licensees within the Degraded Security Cornerstone.
0	Total number of licensees within the Repetitive Degraded Cornerstone.
0	Total number of licensees with Unacceptable Performance.

VI FOF Inspection

Evolution of FOF Inspections

The NRC phased in the enhanced FOF program over a 2-year period in conjunction with testing 56 percent of the commercial NPPs in the country. The first phase consisted of an expanded table-top program conducted in 2002 at seven NPP sites. The second phase, an expanded pilot FOF exercise program, began in February 2003 and was conducted at 15 NPPs. The second phase incorporated lessons learned from the expanded table-top program.

This pilot FOF program assessed the post-9/11 program changes that included additional participants; enhanced weaponry; more complex tactical approaches and protective strategies; increased attention to adversary approach, capture, and destroy tactics; and state-of-the-art exercise equipment. Additionally, one site conducted training exercises beyond the DBT with

incrementally larger numbers of adversaries and enhanced weaponry. The licensees that participated in the FOF pilot program were pre-selected to represent a reasonable sampling of the various designs, locations, number of responders and size of facility.

In February 2004, the NRC began the final phase, starting with a transitional force-on-force (TFOF) program, that incorporated lessons learned from the previous 2 years. The TFOF mock adversary force used the characteristics of the DBT, as enhanced and supplemented by NRC Orders, that had expanded adversary force capabilities. A total of 13 sites had participated in the TFOF program by October 2004.

In November 2004, NRC began implementation of its redesigned, full-scale FOF inspection program that incorporates experience and lessons learned since September 11, 2001. The NRC has increased the frequency of FOF inspections so that each nuclear power plant site participates in one NRC-conducted FOF inspection (which typically includes three NRC-evaluated exercises) at least once every 3 years, rather than once every 8 years. In addition, each plant is required to conduct its own independent exercise (tactical response security exercises) at least once a year. The conduct of these licensee tactical response security exercises are subject to NRC oversight. The current FOF program reflects the supplemented DBT for radiological sabotage and significantly increases the level of realism, while ensuring NRC licensees are meeting regulatory requirements. Lastly, during 2004, the NRC enhanced its oversight of licensee security equipment performance testing and maintenance; protective strategy and severe accident management; fitness for duty; information and technology security; and physical protection of shipments of nuclear material.

In conducting FOF inspections, NRC notifies the licensee in advance for safety and logistical purposes. This notification provides adequate planning time for licensee coordination of two sets of security officers - one for maintaining actual plant security and the other for participating in the exercise. In addition, arrangements must be made by the licensee for a group of individuals who will control and monitor each exercise. A key goal of the NRC is to balance safety (both personnel and operational), while maintaining actual plant security during an exercise that is as realistic as possible.

In preparation for a FOF inspection, information from table-top drills, other baseline security inspections, and security plan reviews are used to design a number of commando-style attack scenarios seeking to probe for potential deficiencies in the licensee's protective strategy. The aim of the site's defenders is to keep the attackers from destroying or damaging (simulated in an FOF exercise) critical equipment (target sets). Any potential deficiencies in the protective strategy identified during FOF exercises are promptly reviewed and corrected before NRC inspectors leave the licensee's site.[8]

The NRC recently clarified that the FOF program does not focus solely on success or failure in protecting critical equipment (target sets), but also identifies licensee performance weaknesses and areas for improvement. This allows the NRC to more reliably assess the capability of a licensee security force to execute an effective protective strategy. The FOF program retains the goal of protecting critical equipment (target sets) and applies the performance assessment

[3] See "Protecting Our Nation," and Office of Public Affairs "Backgrounder" on Force-on-Force.

tools and techniques. This philosophy comports with the principles of the NRC ROP and is more effective in both assessing and improving licensee performance.

Qualification of FOF Inspectors

In order to meet the needs of an accelerated inspection schedule, the NRC had to increase staffing levels. The NRC recruited and hired security specialists with substantial experience from outside the agency, including industry, law enforcement, and the military. Throughout 2004, the FOF inspection team members completed various training courses, self-study programs, and NPP site visits. Each inspector was required to sit before an oral qualification board to demonstrate his or her knowledge of the regulatory and inspection processes, required as part of the NRC's inspector qualification program. Team members were certified as interim inspectors prior to November 2004, awaiting attendance of additional training courses and on-the-job training. Inspectors continue to enhance knowledge of the latest trends and advances in security and increase their understanding of reactor systems.

Exercise Simulation Systems (ESS)

As one of the ongoing enhancements to improve the realism of FOF exercises, the NRC incorporated Multiple Integrated Laser Engagement System (MILES) equipment into the exercises. With MILES, transmitters are mounted to the weapons, which emit lasers when blank cartridges are fired. Sensors attached to the exercise participants detect the laser, and determine if that player is "neutralized." Prior to the integration of MILES into the FOF program, responders would engage using "red guns" or mock weapons carried and aimed like real weapons. Exercise controllers would determine the outcome of engagements by considering factors such as distance, use of cover and concealment, and number of shots fired. Considerable artificialities were introduced to the evaluation with this engagement method. When used properly and with sufficient training, MILES equipment provides a much greater degree of realism and reduces many artificialities of simulated combat.

In order to ensure use of MILES equipment at all FOF inspections, the NRC acquired its own dedicated MILES 2000 equipment which is maintained by the Department of Energy/National Nuclear Security Administration (DOE/NNSA). DOE contractors transport the equipment to each site and are responsible for distribution of the equipment and blank ammunition to each security responder and adversary. These contractors, along with the NRC inspection team, are important components of maintaining a safe and realistic exercise environment.[9]

An additional benefit of the MILES equipment maintained by DOE/NNSA is the After Action Review capability. Data is downloaded from each exercise participant's harness and can be formatted into a spreadsheet to concisely summarize the engagement outcomes.

If a licensee provides its own MILES, or equivalent ESS equipment, it may be used in lieu of the NRC-provided MILES equipment if it: functions reliably; has comparable operational and safety features to the NRC-provided MILES equipment; and is operated in accordance with written guidance for the use and training of MILES equipment that, at a minimum, is equivalent to the

[4] "Protecting Our Nation."

guidance used with NRC-provided MILES equipment. Prior to conducting FOF inspections, inspectors verify that the licensees meet the established performance and safety requirements in accordance with the inspection procedure and regulatory guidance. Through the end of CY 2005, three sites have used their own MILES or ESS equipment.[10]

Composite Adversary Force

A credible, well-trained, and consistent mock adversary force is vital to the NRC's FOF program. Previously, power plant operators had assembled adversary teams that frequently included security officers from their own sites, other licensees, and state police tactical team members. However, using these diverse sources caused inconsistencies in the capabilities of the adversary team.

To improve the program, the NRC worked with the nuclear industry to develop a composite adversary force (CAF) that is trained to standards issued by the Commission. The new adversary force has been used for all FOF exercises conducted after October 2004. The CAF has proven to be a significant improvement in ability, consistency, and effectiveness over the previous adversary forces. The CAF is evaluated at each exercise using NRC performance standards issued in April 2004. To date, the CAF has met the expectations of the NRC.

The CAF is primarily made up of employees from and managed by a company (The Wackenhut Corporation (TWC)) that provides much of the security for U.S. nuclear power plants and is, therefore, well-versed in the security operations of power plants. The NRC recognizes that there may be a perception of a conflict-of-interest where the management company cannot adequately test either the CAF or the plant security force. NRC established expectations for a clear separation of functions within TWC and between the CAF and plant security forces to ensure an independent, reliable, and credible mock adversary force. In addition, no member of the CAF may participate in an exercise at his or her home site. These measures in aggregate, serve to mitigate any potential conflict of interests as required by Section 651 of the Energy Policy Act of 2005.

It is important to emphasize that the NRC designs, runs, and evaluates the results of the FOF exercises. The NRC establishes the exercise objectives, boundaries, and timelines, and the NRC and its contractors continually observe the performance of the CAF. The CAF carries out the planned mock attacks, under the direction and guidance of the NRC. Should industry be unable to maintain an adequate and objective CAF that meets the standards mandated by the NRC, the NRC will take the necessary actions to ensure the effectiveness of the FOF evaluation program.[11]

To date, there have been two complete CAF graduating classes, and three abbreviated classes to supplement membership. Currently, the CAF consists of 73.3% TWC members, and 26.7% non-TWC members. The contract ensures adequate non-TWC representation on the CAF.

---

[5] Inspection Procedure 71130.03, "Contingency Response Force-on-Force Testing," issued December 30, 2005.

[6] Office of Public Affairs "Backgrounder" on Force-on-Force.

Inspection Procedure 71130.03 Revision

Throughout the first year of FOF inspections, the staff compiled lessons learned regarding both the staff and licensees. Those lessons learned were subsequently fed back to all of the inspection teams, as well as licensees and industry representatives to increase regulatory stability and to ensure consistency throughout the inspections. FOF Inspection Procedure 71130.03, "Contingency Response Force-on-Force Testing," was revised and issued on December 30, 2005, to reflect process improvements and the lessons learned from the previous year. Staff continues to compile lessons learned and will update the inspection procedure and other regulatory guidance as needed.

Improved Controller Training and Qualification

Controllers are a vital part of conducting safe and realistic FOF inspections. They are stationed with on-duty forces and with mock player forces, ensuring that live weapons carried by the on-duty forces are controlled during the exercise, that no live ammunition is brought into the exercise field, and that the proper engagement determinations are made in an event where the use of MILES may not be appropriate or situations when equipment malfunctions. In 2004, the Commission directed the staff to work with industry to voluntarily implement improved controller training and qualification. Since then, NRC staff has worked with the industry's Nuclear Security Working Group (NSWG) on the NRC's expectations for such improved training and qualification. As of the issuance of this report, industry has drafted a proposal for improved controller training and qualification for NRC endorsement.

Throughout the first year of inspections, staff has observed varying degrees of consistency among licensee controllers. At one site, insufficient controller qualification caused exercise results to be indeterminate. At other sites, NRC staff was able to validate the protective strategy, despite controller performance issues. NRC recognizes the importance of improved controller training and qualification, and is working to resolve recurrent issues with controllers. The Commission has directed staff to develop Orders to be issued to any licensee who does not voluntarily implement an improved training and qualification plan for controllers.

Beyond the DBT and Technical Approaches to Beyond DBT

One of the ongoing enhancements to the FOF program is the planned integration of beyond-DBT exercises. In late 2005, the Commission directed the staff to begin formally integrating beyond-DBT testing into the FOF program on a voluntary basis for licensees, beginning with the Joint Conflict and Tactical Simulation (JCATS) system.

JCATS is a Department of Defense (DOD) tool, developed by the Lawrence Livermore National Laboratory, for simulating joint military exercises. It is also a useful tool for analyzing and improving physical security. With its ability to model individual buildings accurately, obstructed lines of sight, the time required to cut through walls or penetrate barriers, as well as its ability to model interactions of individual entities, JCATS is well suited for evaluation of NRC licensees.

Since the middle of CY 2005, the NRC has been working with a DOD contractor to build site models for each power reactor and CAT I fuel facility. The basic site models, which include terrain features and building shells, have been completed for all power reactor and CAT I facilities. In February 2006, staff demonstrated JCATS to the Commission, running scenarios with fully completed models, including security features, fencelines, building floorplans, target

set components, and unique adversary and responder characteristics. At the time of this report, the staff has fully completed site models for one reactor and one CAT I facility. In FY 2006, staff will selectively enhance site models, and will begin to plan for the integration of JCATS into the FOF program.

The Commission has also directed the staff to explore beyond-DBT testing for training in FOF exercises by incrementally increasing numbers of adversaries. This beyond-DBT testing could potentially be incorporated as an initiative completely separate from the inspection program, or by substituting a beyond-DBT scenario for the third exercise of the inspection. The licensee would only be given the option to substitute the third exercise with a beyond-DBT training exercise provided that the protective strategy was demonstrated successfully, with margin, in the first two exercises.

Indeterminate Exercise

NRC management will make the determination when less than three exercises are acceptable. This determination will be contingent upon: (1) at least two exercises having been conducted; (2) both exercises having successfully demonstrated an effective protective strategy; and (3) no significant issues being identified. If those conditions are not met, the team may have to expand the schedule or schedule a subsequent visit. If an exercise is deemed indeterminate or is canceled due to severe weather, CAF management will wait for NRC confirmation before leaving the site. NRC management will make the determination if the CAF team and NRC inspection team will remain on site for any additional days to complete a third exercise. For a licensee to demonstrate an effective protective strategy successfully, there must be a sufficient number of armed responders, bearing the appropriate weapons, in protected positions, arriving in time to neutralize a potential threat. Furthermore, the security force must know what to protect, have a strategy for protecting those assets, and execute the strategy accordingly.

During a FOF inspection, a minimum of three FOF exercises are scheduled. However, due to circumstances beyond the control of the on-site NRC inspection team, an exercise may have to be canceled. For example, severe weather may result in an exercise being canceled due to personnel safety considerations. There are occasions, when the NRC inspection team determines that an exercise may be deemed “indeterminate.” An indeterminate exercise is one where the NRC inspectors are prevented from effectively gathering sufficient information to evaluate the licensee’s protective strategy or to form a cogent conclusion. Examples of indeterminate exercises include, but are not limited to; excessive safety or administrative holds, insufficient exercise control, or extreme malfunctions of ESS equipment.

VII FOF Regulatory Program Activities

Between October 29, 2004 and December 31, 2005, FOF inspections were conducted at 21 sites. One site was revisited during that time period, 5 months after the original FOF inspection, because of performance issues. The first week of inspection activities was completed at one site in August 2005, but the exercise week was postponed due to the impact of Hurricane Katrina in the region. The inspection will be completed in the near future. An inspection at another NPP included an additional exercise being observed by NRC management and staff, after performance issues occurred during the FOF inspection.

From all of the inspections in this reporting period of the redesigned FOF program, there were three findings. Table 2 below summarizes the first 23 inspections.

Table 2 - CY 2005 FOF Inspection Program Results

Findings	Number of Facilities	Basis
No findings	18	N/A
Green NCVs	3	Inadequate Target Set Development Controller issues Performance Deficiencies During Exercise 1
Greater than Green	0	N/A
SL IV	0	N/A
Greater than SL IV	0	N/A
Rescheduled	1	Hurricane Katrina
Inspection Open	1	Findings under review

VIII FOF 2006 Planned Activities

FOF inspections are scheduled for 24 sites in CY 2006, including two Category I fuel cycle facilities, one inspection at a site that was delayed due to Hurricane Katrina.

IX Disposition of Findings

Following the terrorist attacks of September 11, 2001, the NRC issued Orders and Confirmatory Action Letters (CAL) containing requirements for compensatory measures enhancing the security function. On September 11, 2003, the Compensatory Measures Management Review Panel (CMMRP) was created to review all security inspection findings and ensure consistent application and resolution of inspection findings. The panel membership includes NRC Management from various NRC offices and the regional offices. In 2005, the panel name was changed to the Security Findings Review Panel (SFRP) to reflect the current status of the panel's efforts to review and ensure NRC consistency for all security related findings, not just findings concerning Commission directed Orders.

As with all security-related findings, findings that result from FOF inspections are reviewed by NRC management in the SFRP. The panel consists of designated representatives from various offices within the NRC as voting members, and others as appropriate to the issue.

The purpose of the SFRP, like its predecessor, the CMMRP, is to ensure regulatory consistency by reviewing and dispositioning findings, URIs, and potential findings resulting from the inspection or observation of any licensees' implementation of 10 CFR regulations, Orders, physical security plans, technical specifications, and Confirmatory Action Letters. For NPPs, this includes any and all findings related to the security cornerstone. Although the panel will review and approve the approach to dispositioning an issue, applicable agency processes will be used prior to issuance of any enforcement action.

X Communications

As part of an effort to improve openness in communicating security information to the public, on April 4, 2006, the Commission approved the recommendation of the staff to increase the amount of public information released pursuant to the implementation of the Security Oversight Process. For security-related inspection reports issued after May 8, 2006, the inspection report cover letters will be released to the public with information of whether or not findings occurred. Guidelines are being developed to facilitate efficient staff assessments of making information available to the public and are expected to be completed by July 2006.

In an effort to improve public awareness and understanding, the NRC has held two public meetings specifically on nuclear security issues in August 2004 and September 2005. Additionally, security topics are presented at the NRC's Regulatory Information Conference, held annually in Rockville, Maryland.

After each inspection, NRC staff gathers lessons learned in a variety of categories, including: safety issues; protective strategy; MILES; CAF; controllers; qualification course of fire; target sets; and exercise functional issues. Through the NSWG, a consortium of security representatives from NRC licensed facilities, lessons learned are shared mutually between the NRC and industry. The NSWG assists in disseminating information to the industry for the combined goal of safe and realistic performance evaluations.

In most FOF inspections, representatives from local law enforcement agencies attend planning activities and observe the exercise to improve understanding of the licensee's response and coordination of integrated response activities. Other representatives from state emergency management agencies, state governments, the Government Accountability Office, Congress and Senate have also frequently observed FOF inspections.

XI Interagency Support

The NRC continues to support the U.S. Department of Homeland Security (DHS)/Homeland Security Council (HSC) initiative to enhance integrated response planning for power reactor facilities. In 2004, two Integrated Response tabletop exercises were completed. The staff is continuing to work with HSC, DHS, Federal Bureau of Investigation (FBI) and others to develop plans to address recommended actions. In addition, the staff is coordinating with other Federal agencies and State and local security partners in the development of Emergency Action Levels for all imminent threats.

XII Reference List

1. NRC, “Backgrounder on Force-on-Force Exercises at Nuclear Power Plants,” http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/force-on-force.html

2. NRC, “Protecting Our Nation,” NUREG/BR-0314, September 2004, http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/

3. NRC, “Weekly Information Report - Week Ending 12/2/05,” ADAMS accession number ML053500054

4. NRC, “Frequently Asked Questions on Force-on-Force Security Exercises at Nuclear Power Plants,” http://www.nrc.gov/what-we-do/safeguards/faq-force-on-force.html

5. Luis Reyes to Danielle Brian, Project on Government Oversight, regarding Composite Adversary Force for Security Drills at Nuclear Power Plants, 9/30/04, http://www.nrc.gov/reading-rm/doc-collections/for-the-record/2004/ltr-to-daniellebrian-pogo.pdf

6. NRC, “Response to Questions about Wackenhut and Public Access to Security Results” http://www.nrc.gov/reading-rm/doc-collections/for-the-record/2004/nsir-response.pdf

7. NRC, “Weekly Information Report - Week Ending 12/2/05,” ADAMS accession number ML053500054.

XIII Acronym List

CAF . . . . . Composite Adversary Force
CAL . . . . . Confirmatory Action Letter
CAT I . . . . . Category I
CFR . . . . . Code of Federal Regulations
CMMRP . . . . . Compensatory Measures Management Review Panel
CY . . . . . Calendar Year
DBT . . . . . Design Basis Threat
DOD . . . . . Department of Defense
DOE . . . . . Department of Energy
DPO . . . . . Differing Professional Opinion
EFOF . . . . . Expanded Force-on-Force
ESS . . . . . Exercise Simulation System
FOF . . . . . Force-on-Force
FY . . . . . Fiscal Year
ISFSI . . . . . Independent Spent Fuel Storage Installation
JCATS . . . . . Joint Conflict and Tactical Simulation
MC&A . . . . . Material Control and Accounting
MILES . . . . . Multiple Integrated Laser Engagement System
NCV . . . . . Non-Cited Violation
NEI . . . . . Nuclear Energy Institute
NNSA . . . . . National Nuclear Security Agency
NPP . . . . . Nuclear Power Plant
NRC . . . . . Nuclear Regulatory Commission
NSIR . . . . . Office of Nuclear Security and Incident Response
NSWG . . . . . Nuclear Security Working Group
PPSDP . . . . . Physical Protection Significance Determination Process
ROP . . . . . Reactor Oversight Process
SDP . . . . . Significance Determination Process
SFRP . . . . . Security Findings Review Panel
TFOF . . . . . Transitional Force-on-Force
TWC . . . . . The Wackenhut Corporation
URI . . . . . Unresolved Item