INSPECTION MANUAL CHAPTER 0308 ATTACHMENT 6

BASIS DOCUMENT FOR SECURITY CORNERSTONE OF THE REACTOR OVERSIGHT PROCESS

Effective Date: 01/01/2021

0308-06-01 INTRODUCTION

The security cornerstone of the Reactor Oversight Process (ROP) was originally called the "physical protection" cornerstone and was developed in the same manner as the other ROP cornerstones. The security cornerstone is intended to meet the same guiding principles and program objectives as the rest of the ROP. Those principles and objectives are described in Inspection Manual Chapters (IMCs) 0305and 0308 and the source documents listed in Section 8.

0308-06-02 CORNERSTONE STRUCTURE AND OBJECTIVE

To understand how the cornerstone of safety is defined for safeguards and how it supports the ROP's objectives and the agency's mission and goals as stated in the NRC's Strategic Plan, refer to the security section in the cornerstones of safety in IMC 0308, "Reactor Oversight Process Basis Document".

Key Attributes and Critical Elements

Through expert panels, key attributes were described for each cornerstone. The key attributes were those areas within a cornerstone that needed to function for the associated licensee program or activity to meet the cornerstone's objective. Within each key attribute, the staff then determined those specific elements (called critical elements) that needed to be verified to determine if the licensee's performance and programs adequately met the key attribute and, therefore, met the cornerstone's objective. The security cornerstone originally had four key attributes:

- Access authorization
- Access control
- Physical protection
- Contingency response

0308-06-03 INSPECTION

The technical basis for the development of the inspection program for commercial power reactors for the security cornerstone is described in IMC 0308 Attachment 2, "Technical Basis for Inspection Program".

Inspectable Areas

The original physical protection cornerstone had four cornerstone-specific inspectable areas: access control, access authorization, response to contingency events, and security plan changes. The scope of several of the inspectable areas was limited because performance indicators were being used to measure aspects of the area and, therefore, those aspects were not directly inspected under the baseline inspection program.

Following the events of September 11, 2001, the U. S. Nuclear Regulatory Commission (NRC) issued additional security requirements on its licensees and created the Office of Nuclear Security and Incident Response (NSIR) to increase oversight of security at its licensees. The NRC also initiated several analyses, evaluations, and studies to determine the vulnerabilities of its licensees to various scenarios and to develop strategies to reduce the vulnerabilities and mitigate the consequences of such scenarios. In addition, the agency revised its list of capabilities for the design basis threat (DBT) against which power reactor licensees must be able to protect their plants. The agency also removed from public access any security-related information that could potentially be of benefit to adversaries wishing to do harm to NRC licensees.

When the agency created NSIR, the NRC included in NSIR's responsibilities the oversight of material control and accounting (MC&A). An additional key attribute, MC&A, and associated critical elements were added to the security cornerstone in 2007. In 2013, the Office of Nuclear Material Safety and Safeguards (NMSS), via memorandum (ML13309A697), assumed the responsibility for oversight of MC&A however, the key attributes and the critical elements continue to remain in the security cornerstone.

0308-06-04 PERFORMANCE INDICATORS

When the ROP was developed, the staff attempted to relate Performance Indicators (PI) thresholds to probabilistic risk data. This was achieved for most/or some of the reactor safety cornerstones. Other PI thresholds could not be specifically tied to probabilistic risk data. In such cases, the PI thresholds were tied to regulatory requirements or were based on the professional judgment of the NRC staff. In the security cornerstone, the PI provides a useful measure of the status of systems, but its thresholds were chosen based on the professional judgment of the NRC staff.

The PIs in the security cornerstone do not have thresholds identified for the Yellow or Red Bands because there is no risk basis for a determination that a certain degraded level of performance reflected by these indicators can be correlated into mandatory plant shutdown. It is expected that declining performance in the area monitored by the indicators would be interrupted by increased licensee corrective actions and by increased NRC attention.

0308-06-05 SIGNIFICANCE DETERMINATION PROCESS

The purpose of the Baseline Security Significance Determination Process (BSSDP) is to provide an objective means of evaluating findings related to common defense and security for activities licensed by the NRC as defined in IMC 2201, "Security Inspection Program for Operating Commercial Nuclear Power Reactors." The process also is used to provide reasonable assurance that licensees' safeguards systems can provide adequate protection against the DBT based on defense-in-depth layers of protection as part of licensees' commitments to NRC requirements. The BSSDP incorporates areas of MC&A, protection of Safeguards Information, and physical protection. The BSSDP is utilized once a performance deficiency has been evaluated as more than minor using IMC 0612, Appendix B, "Issue Screening," and determined to be in the security area in accordance with IMC 0609, Attachment 4, "Initial Characterization of Findings."

0308-06-06 PUBLIC ACCESS TO INFORMATION

In November 2003, the Commission asked the staff to present it with options for addressing the security cornerstone of the ROP. The staff sent the Commission several options (see SECY-04-0020) with no change to the then current process and ending with a completely different process for assessing security. The Commission chose an option that kept the security cornerstone in the ROP, but assessed security separate from the other ROP cornerstones. The Commission specifically directed the staff to "make no information publicly available" (see SRM-SECY-04-0020).

The staff implemented the Commission's direction in August 2004, by removing from the NRC's public web pages the ROP assessment information related to the security cornerstone and making non-safeguards, security-related inspection documents official use only. At the time, no security-related inspection reports or their cover letters were public because of an earlier response to the events of September 11, 2001. However, in July 2011, the Commission approved staff's proposal to "reintegrate security inspection findings and PIs into the Action Matrix of the ROP for commercial nuclear power licensees." The Commission also approved the staff's recommendation "that the proposal be considered, where applicable and appropriate, for other NRC security inspection and oversight programs, such as reactors under construction" (see SRM-SECY-11-0073).

Also, by Commission direction (see SRM-04-191), the staff later provided new options to make certain information about security inspections publicly available. The Commission chose an option that would identify that a security inspection had been performed and that findings had been identified. However, the Commission directed the staff to make public only certain, limited information regarding the inspections and associated findings. Details regarding the nature of any findings as well as the number findings that were greater-than-green in significance were withheld from public disclosure.

0308-06-07 REFERENCES

7.1 Commission Papers and Staff Requirements Memoranda

SECY 99-007, “Recommendations for Reactor Oversight Process Improvements” (ML992740074) (non-public)

SECY 99-007A, “Recommendations for Reactor Oversight Process Improvements Follow up to Secy-99-007)” (ML992740073) (non-public)

SECY-04-0002, “Revisions to the Power Reactor Physical Protection Baseline Inspection Program” (ML033390092) (non-public)

SECY-04-0020, “Treatment of Physical Protection Under the Reactor Oversight Process” (ML033570084) (non-public)

SRM-SECY-04-0020, "Treatment of Physical Protection Under the Reactor Oversight Process" (ML040900126) (non-public)

SECY-04-0091, “Provisional Physical Protection Determination Process to evaluate Findings from the Security Baseline Inspection and Force-on-Force Inspection Programs” (ML040130797) (non-public)

SRM-SECY-04-0191, “Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure” (non-public)

SECY-05-0082, “Revised Assessment Process for the Security Cornerstone of the Reactor Oversight Process” (ML051090579) (non-public)

SRM-SECY-05-0082, “Revised Assessment Process for the Security Cornerstone of the Reactor Oversight Process” (ML052280031) (non-public)

SECY-05-0107, “Status of Activities and Improvements to the Physical Protection Significance Determination Process” (ML051640574) (non-public)

SECY-06-0036, “Public Disclosure Options within the Security Cornerstone of the Reactor Oversight Process” (non-public)

SECY-07-0015, “Results of Trial Assessment of the Industry's Optional Physical Protection Significance Determination Process” (ML070080171) (non-public)

SECY-07-0136, “Recommendation to Discontinue Two of Three Performance Indicators Associated with The Security Reactor Oversight Process,” (ML062760640) (non-public)

SRM-SECY-07-0136, “Recommendation to Discontinue Two of Three Performance Indicators Associated with The Security Reactor Oversight Process,” (ML072560811) (non-public)

SECY-11-0073, “Staff Proposal to Reintegrate Security into the Action Matrix of the Reactor Oversight Process Assessment Program” (ML112020038) (non-public)

SECY-16-0073 (ML17223A335), “Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SEC-14-0088 (ML16279A345).” (non-public)

7.2 Program Documents

(Note: a full list of ROP-related program documents can be found at http://www.nrc.gov/reactors/operating/oversight/program-documents.html)

Inspection Manual Chapter (IMC) 0305, “Operating Reactor Assessment Program”

IMC 0308, “Reactor Oversight Process Basis Document”

IMC 0609, “Significance Determination Process”

IMC 0609, Appendix E, “Physical Protection Significance Determination Process for Power Reactors”

IMC 2201, “Security and Safeguards Inspection Program for Commercial Power Reactors”

7.3 Non-NRC Documents

Nuclear Energy Institute NEI-99-02, “Regulatory Assessment Performance Indicator Guideline,” Revision 7, 31 August 2013

Figure 1: Access Authorization Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Access Authorization	
Cornerstone: Security	Inspection Procedure: 71130.01
Scope: To verify the licensee is properly implementing its personnel screening and fitness-for-duty (FFD) programs, including granting, denying, and revoking unescorted access authorization into the protected area, as appropriate, as well as verifying all other applicable areas of access authorization are being properly implemented. The frequency at which this inspection activity is to be conducted is triennially (once every three years).	
Basis: Inspection of this area supports the Security Cornerstone. This is a risk-significant area because the personnel screening and FFD processes are used to verify personnel reliability and trustworthiness prior to granting unescorted access to the site protected and vital areas, and to assure continued reliability and trustworthiness throughout the period of unescorted access and authorization. The establishment of reliability and trustworthiness for persons granted unescorted access to the protected area is a major component of protection against the insider threat of radiological sabotage as defined in 10 *Code of Federal Regulations* (CFR) 73.1. The behavioral observation process is used to monitor the continuation of trustworthiness for persons authorized unescorted access and for escorted visitors. An individual with malevolent intent or an individual under the influence of drugs could be granted unescorted access due to human or program failure. The frequency of this type of event has been low but the safety significance of this type event can be medium to high. The probability of a single individual causing a radiological release is low although the consequences of an individual causing a radiological release can be high depending on the individual's knowledge of plant systems. Historically, licensees have effectively implemented the personnel screening and FFD programs. The licensee is required by 10 CFR 73.56 to maintain an access authorization program, which includes background investigations and psychological assessments, for granting individuals unescorted access to protected and vital areas with the objective of providing reasonable assurance that the individuals are trustworthy and reliable and do not constitute an unreasonable risk to public health and safety including the potential to commit radiological sabotage. The licensee is also required by 10 CFR 26.10 to maintain an FFD program that provides reasonable assurance that the workforce will perform tasks in a reliable and trustworthy manner and that they are not under the influence or impaired from any cause. Both rules require behavioral observation to detect indications of behavioral problems that could constitute a threat to public health and safety.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2004: SECY-04-0002 revised security baseline inspection program, broadening the scope of this area. 2007: SECY-07-0136 removed the two security PIs that affected this inspectable area as the area is now fully inspected.	

Figure 2: Access Control Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Access Control	
Cornerstone: Security	Inspection Procedure: 71130.02
Scope: To verify that the licensee has effective access controls and equipment in place designed to detect and prevent the introduction of contraband (firearms, explosives, incendiary devices) into the protected area that could be used to commit radiological sabotage and to assure that only authorized personnel are permitted unescorted access to the site protected area and vital areas. The Identification and Authorization process are to ensure that, once personnel have been screened to verify their trustworthiness and reliability, those persons have a need for access and to confirm that only those persons who have been screened and have a need are granted access to the plant including vital areas. Some of the equipment involved in the search process are metal detectors, explosive detectors, x-ray machines, biometric sensors, computers, key-cards, hard keys, and card-readers. The frequency at which this inspection activity is to be conducted is annyally (once per calendar year).	
Basis: Inspection of this area supports the Security Cornerstone. The areas to measure are the effectiveness of the search (personnel, packages and vehicles) and the identification and authorization functions. The search function is to prevent the introduction of contraband (firearms, explosives, incendiary devices) that could be used to commit radiological sabotage. The search function for detection of firearms, explosives and incendiary devices on individuals, in packages, or vehicles, is accomplished by equipment and/or a hands-on search. The identification and authorization functions are accomplished during issuing of badges and through using biometrics or card-readers. The licensee must also positively control all points of personnel, material and access into the protected areas.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2004: SECY-04-0002 revised security baseline inspection program, broadening the scope of this area in response to the NRC's comprehensive review following September 11, 2001.	

Figure 3: Contingency Response Force-on-Force Testing Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Contingency Response Force-on-Force Testing	
Cornerstone: Security	Inspection Procedure: 71130.03
Scope: Verify that the licensee has the capability to protect its target sets against the design basis threat. The implementation of the protective strategy includes demonstrating that the strategy works, and that the security force can successfully protect against the design basis threat through drills and exercises. The frequency at which this inspection activity is to be conducted is triennially (once every three calendar years). Scope: Verify that the licensee has the capability to protect its target sets against the design basis threat. The implementation of the protective strategy includes demonstrating that the strategy works, and that the security force can successfully protect against the design basis threat through drills and exercises. The frequency at which this inspection activity is to be conducted is triennially (once every three calendar years).	
Basis: Inspection of this area supports the Security Cornerstone. This is a high risk-significant system necessary to protect against the design basis threat of radiological sabotage. The licensee should be able to demonstrate the ability to respond with sufficient force, properly armed, appropriately trained and within the appropriate time protected positions in order to interdict and neutralize the design-basis adversary force to protect target sets necessary for the safe shutdown of the plant. The ability of the security force to effectively respond to the design basis threat is contingent upon the number of armed responders team personnel committed to in the physical security plan; the intrusion detection system being able to detect; the alarm status being communicated to the alarm stations; the assessment functions (closed-circuit television and lighting) and the training of central alarm station and secondary alarm station operators, communications on and off site, the response officers and response team leaders, including handling and qualification with assigned weapons, and the use of proper tactics. Each of these items will be reviewed to determine if they can perform their intended function against the design basis threat and as identified in the Security Plan (Physical, Contingency, Training and Qualified).	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2000: Operational Security Response Evaluation (OSRE) force-on-force drills are conducted per IP 81110, "Operational Safeguards Response Evaluation (OSRE)." 2002: SECY-02-0104, comprehensive review. The staff explored ways to resume force-on-force exercises in a manner that will evaluate the licensee's ability to meet existing requirements, including the interim compensatory measures (ICMs), while gaining insights to inform the revision of the power reactor DBT and the completion of the vulnerability assessment. 2002-2004: The staff piloted and then expanded a force-on-force program that could be incorporated into the routine oversight of nuclear power reactors. This expansion included the use of trained controllers, use of NRC supplied laser-engagement weapon platform	

systems, minimizing artificialities, credible, realistic challenges to the protective strategies and the use of a mock adversary force.

November 2004: The inspectable area attachment was rewritten to make the force-on-force exercises a routine part of the NRC's inspection oversight considering September 11, 2001. This IP was changed from a biennial, non-force-on-force inspection to a triennial force-on-force exercise inspection conducted by NSIR headquarters.

2014 FOF program revised from three exercises to two exercises.

Figure 4: Equipment Performance, Testing and Maintenance Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Equipment Performance, Testing and Maintenance	
Cornerstone: Security	Inspection Procedure: 71130.04
Scope: Critical security system and intruder detection equipment. The frequency at which this inspection activity is to be conducted is biennially (once every two years).	
Basis: Inspection of this area supports the Security Cornerstone. The functionality, reliability, and sensitivity of security system equipment are critical to the effective implementation of a plant's security program.	
Performance Indicator(s): The Protected Area Security Equipment Performance Index affects this inspectable area, as this procedure inspects the availability of the PA boundary. However, no reduction in scope of inspection is made for the PI. See the PI's basis summary sheet, Figure 10, below.	
Significant Changes in Scope or Bases: 2004: SECY-04-0002 revised security baseline inspection program, broadening the scope of this area in response to the NRC's comprehensive review following September 11, 2001.	

Figure 5: Protective Strategy Evaluation and Performance Evaluation Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Protective Strategy Evaluation and Performance Evaluation Program	
Cornerstone: Security	Inspection Procedure: 71130.05
Scope: To verify that the plant's protective strategy remains effective. Review site security plans and associated procedures and licensee conducted drills and exercises. The frequency at which this inspection activity is to be conducted is triennially (once every three years)	
Basis: Inspection of this area supports the Security Cornerstone. An effective protective strategy is necessary to ensure safety of a plant during an attack by a design-basis threat-level force. Therefore, it is an important aspect of the licensee's contingency response. The ability of the security force to effectively respond to the design basis threat is contingent upon the number of armed response team personnel committed to in the physical security plan, the intrusion detection system being able to detect, the alarm status being communicated to the alarm stations, the assessment functions (closed-circuit television and lighting) and the training of central alarm station and secondary alarm station operators, communications on and off site, the response officers and response team leaders, including handling and qualification with assigned weapons, and the use of proper tactics. Each of these items will be reviewed to determine if they can perform their intended function against the design basis threat and as identified in the Security Plan (Physical, Contingency, Training and Qualified). The comprehensive review following September 11, 2001, and the additional requirements imposed by orders broadened the scope of areas the NRC determined it needed to verify through its baseline inspection program.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2004: SECY-04-0002 added the force-on-force inspectable area (71130.03) into the program in response to September 11, 2001, and this inspectable area was expanded and renumbered as 71130.05. 2014: Inspection procedure revised to include observation of licensee-conducted annual force-on-force exercise.	

Figure 6: Security Training Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Security Plan Changes	
Cornerstone: Security	Inspection Procedure: 71130.06
Scope: Initial training and periodic requalification training, including weapons training. The frequency at which this inspection activity is to be conducted is biennially (once every two years). Scope: Inspection activities in this area focus upon those changes made by a licensee to the site Physical Security Plan, Safeguards Plan, or Training and Qualification Plan without prior Commission approval under the provisions of 10 CFR 50.54 and those changes to the facility, procedures, tests or the Updated Final Safety Analysis Report (UFSAR) performed under the requirements of 10 CFR 50.59. The inspection activities include a review of the documentation submitted by a licensee as specified by 10 CFR 50.54 and 50.59. A more detailed review would be performed on those changes made without prior Commission approval where a decrease of effectiveness has or could have resulted from the change or on those changes that have the potential to be and/or appear to be intent changes. Examples of inspection areas would include safety evaluations performed by the licensee for permanent and temporary facility modifications, procedure changes, UFSAR changes, emergency and security plan changes.	
Basis: Inspection of this area supports the Security Cornerstones. Effective implementation of a licensee's protective strategy and effective defense against the design basis threat depends on having properly training and qualified security officers who are properly equipped. The comprehensive review following September 11, 2001, and the additional requirements imposed by orders broadened the scope of areas the NRC determined it needed to verify through its baseline inspection program. The scope was broadened to include educating and raising awareness of personnel to respond to postulated attacks.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2004: SECY-04-0002 added this inspectable area into the program in response to September 11, 2001.	

Figure 7: Fitness-for-Duty Program Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Fitness-for-Duty Program	
Cornerstone: Security	Inspection Procedure: 71130.08
Scope: An initial inspection of the full scope of the licensees' programs, then periodic inspections of program changes. The frequency at which this inspection activity is to be conducted is triennially (once every three years).	
Basis: Inspection of this area supports the Security Cornerstone. Protection and defense against the design basis threat requires that the licensee's staff not be impaired in performing their assigned duties. The comprehensive review following September 11, 2001 and the additional requirements imposed by orders broaden the scope of areas the NRC determined it needed to verify through its baseline inspection program. This area was broadened by adding areas to be inspected. SRM-SECY-07-0136, dated September 13, 2007, recommended that the FFD PI be discontinued because the aspects of security programs measured by the PI are assessed by the BIP, and that this redundancy challenged efficiency and caused undue regulatory burden. Further, the data gained, and insights provided by the PI (1) have been of limited additional value to the security ROP and (2) are already reported to the NRC through 10 CFR reporting requirements.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2004: the inspectable area is added to the cornerstone's baseline inspection program. August 2007: SECY-07-0136 removed the FFD/Personnel Reliability Program PI from the security cornerstone.	

Figure 8: Information Technology Security Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Information Technology Security	
Cornerstone: Security	Inspection Procedure: 71130.10
Scope: This area will verify that the licensee has effectively implemented its cyber security plan and adequately protects digital computers, communication systems, important to safety, security, and emergency preparedness (SSEP) functions from cyber-attacks. The frequency at which this inspection activity is to be conducted is triennially (once every three years).	
Basis: Establishing a cyber security program and implementing a cyber security plan is important in maintaining the digital security of SSEP functions. The following cyber security plan components make up a comprehensive cyber security program; 1) Establishing and Implementing a program 2) Boundary Protection 3) Portable Media Protection 4) Personnel Security 5) Maintenance 6) Training 7) Digital Access Controls 8) Audit and Accountability 9) Communications Protection 10) User Identification and Authentication 11) System Hardening and Detection/Response 12) System Integrity (Protection against Malicious Code) 13) Physical Protection and Physical Access Control 14) Defense in Depth 15) Attack Mitigation and Incident Response 16) Continuity of Operations 17) Configuration Management 18) Acquisition and Supply Chain	
Performance Indicator(s): None	
Significant Changes in Scope or Bases: Publication of 10 *Code of Federal Regulations* 73.54 (“Protection of digital computers, communication systems, and networks”) in 2009, requires nuclear power plant licensees to establish a cyber security program and implement a cyber security plan.	

Figure 9: Material Control and Accounting Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Material Control and Accounting	
Cornerstone: Security	Inspection Procedure: 71130.11
Scope. The scope of this key attribute is verifying the effectiveness of records, procedures and physical inventories used to control and account for special nuclear materials (SNM) at nuclear power plants. This inspection procedure is to be conducted triennially (once every three years), to verify the completeness of SNM records and reports, the adequacy of program and procedures, and the accurate conduct of physical inventory of SNM.	
Basis: Inspection of this area supports the Security Cornerstone. Protection against the loss or misuse of special nuclear material (SNM), i.e., enriched uranium or plutonium, is a critical function of a plant's security program. MC&A works in concert with physical protection to complete the Security Cornerstone with MC&A providing a record of the quantity and location of SNM at the facility, while physical protection protects the facility and the SNM located there. MC&A provides for the timely detection of loss, theft or diversion of SNM. The inspection in this key attribute of the security cornerstone and is used to assess the effectiveness of the licensee's program for control and accounting of SNM. The factors that decrease the risk of loss of SNM are: (1) developing, maintaining and implementing appropriate procedures; (2) generating and maintaining records; and (3) conducting physical inventories. In 1988, the MC&A inspections were changed from "routine" to "as needed" in the IMC-2515 Inspection Program. Beginning in 2004, due to a licensee's loss of two fuel rods, the MC&A inspections were conducted under a three-phase temporary instruction (TI 2515/154, Material Control and Accounting at Nuclear Power Plants and Wet Storage Sites). The results of these inspections were documented in SECY 08-0005, "Results of Material Control and Accounting Baseline Inspections Conducted at Nuclear Power Reactors and Wet Storage Sites." In SECY-05-0082, the staff indicated that MC&A would be added as a key attribute to the Security oversight program because of the importance of control of radioactive material to national security, the identification of unaccounted for fuel pieces, and the integration of materials safety and security in the agency's strategic goals. In response to Commission direction, MC&A was added to the IMC-2201 Security baseline inspection program. At the same time, the Physical Protection Significance Determination Process (SDP) was revised to include MC&A and renamed the Baseline Security SDP. Enforcement history, inspection experience, and expert judgment were used in the development of the MC&A portion of the Baseline Security SDP.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: 2005: SECY-05-0082 stated that MC&A would be added as a key attribute to the security cornerstone. 2007: Exhibit 11 to IMC 0308 was revised in November 2007 to include this key attribute. 2008: IMC 0320 incorporated MC&A as a key attribute to the cornerstone.	

Figure10: Security Aspects Performance Indicator Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Security Performance Index	
Cornerstone: Security	Inspection Procedure: 71151
Scope: The PI is used to monitor security equipment unavailability of the perimeter intrusion detection system. The PI also promotes good practices. Although the NRC is actively overseeing the security cornerstone, the Commission has decided that the description of this PI and its results will not be publicly available to ensure that potentially useful information is not provided to a possible adversary. This inspection procedure is to be conducted annually.	
Basis: This PI was developed and agreed to by an expert panel composed of NRC and industry representatives, based on the collection and review of historical data.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: August 2007: SECY-07-0136 removed two of the three security PIs because the 2004 revision to the security baseline inspection program now inspects those aspects of security that had been reported by the PIs. Although the baseline inspection program now inspects the aspects of security that this PI also measures, the NRC has kept this PI in the program because of its promotion of good practices.	

Figure 11: Review of Power Reactor Target Sets Basis Summary Sheet

BASIS SUMMARY SHEET	
Inspectable Area: Review of Power Reactor Target Sets	
Cornerstone: Security	Inspection Procedure: 71130.14
Scope: Verify that (1) the licensee has developed, revised as necessary, and is implementing a process to identify, document, and maintain site specific target sets to inform the site's protective strategy, (2) a sample of the licensee's complete and accurate target sets includes consideration of cyber-attacks and cyber critical digital assets (CDAs) in documented target sets, and (3) that the licensee includes review of target sets as an element of the physical protection program review as required by Title 10 of the *Code of Federal Regulations* 73.55(m). The frequency at which this inspection activity is to be conducted is triennially (once every 3 years).	
Basis: Inspection of this area supports the Security Cornerstone. The development and maintenance of complete and accurate target sets is necessary to identify which plant structures, systems, and components need to be protected to prevent significant core damage and spent fuel sabotage, which serve as the primary basis for the development of the site's protective strategy. If complete and accurate target sets are not developed and maintained, a site's protective strategy might not be effective against the design basis threat.	
Performance Indicator(s): None.	
Significant Changes in Scope or Bases: March 2013: Revision 2 removed information regarding Part 100 releases which is no longer considered in the Significance Determination Process and included updated information regarding cyber aspects to target sets and spent fuel pools. August 2013: Revision 3 to IP 71130.14 is a complete re-write and was issued to revise the procedure to only inspect the changes since the last target set inspection and a small sample of target sets for completeness and accuracy.	

REVISION HISTORY FOR IMC 0308 ATTACHMENT 6

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Accession Number (Pre-Decisional, Non-Public Information)
N/A	ML081480024 09/08/09 CN 09-021	Initial issuance separating the basis for the security cornerstone from the rest of the ROP because of information sensitivity.	N/A	ML091380039
	ML19116A201 11/09/20 CN 20-061	Periodic update, incorporated regional comments and updated the formatting to current IMC-0040 standards. Updated Basis Summary Sheets, including rewrite of Figure 8, Information Technology Security (Cyber Security); and added Figure 10, Security Performance Index. Completed a SUNSI review and concluded that this document does not need to be controlled. Consistent with the staff's SUNSI determination, SUNSI markings were removed.	N/A	ML19233A213