Reactor Oversight Process Enhancement Project
Baseline Inspection Program
Inspection Area – Safeguards

Background

The most recent iteration of the security baseline inspection procedures (IPs) for the 71130 series was issued in Calendar Year (CY) 2010. The objective of the security baseline inspection program is to gather information to determine whether a licensee is meeting the security cornerstone objective, which is to provide assurance that the licensee's security system and material control and accounting (MC&A) program can protect against the design basis threat of radiological sabotage, and the theft or loss of special nuclear material. The fifth triennial Reactor Oversight Process (ROP) inspection cycle concluded at the end of CY 2013. This marked the end of the ROP inspection cycle for the security baseline inspection program and its associated IPs.

In CY 2013, the ROP Enhancement Project began with the evaluation of each security program IP.

Analysis

During the analysis of the security baseline inspection program, data from the ROP realignment effort was utilized to inform subject matter experts and better prepare them in providing feedback on potential revisions that could increase flexibility, efficiency, and better align inspection resources. Additionally, there were discussions concerning how security fits into the aging management program and engineering inspections.

The Agency also solicited external stakeholder input regarding the baseline inspection program. Key areas in the security baseline inspection program that were analyzed following external stakeholder input were: (1) the potential for redundant inspection requirements found in different IPs; (2) the perception that there is too much engineering judgment in the cyber security inspection procedure (Milestone 8); (3) the way MC&A inspections are scheduled; and (4) the request for increased openness in the assessment process for security findings.

Recommendations

Prior to CY 2014, security IPs did not provide the flexibility to conduct inspections through minimum, nominal, or maximum sampling. Security inspections had been conducted by completing the maximum number of samples or inspection sample requirements regardless of licensee performance. The security baseline inspection procedures have since been revised to incorporate the Office of Nuclear Reactor Regulation's approach to implementing inspections as it pertains to a sampling program, and to establish a minimum, nominal, and maximum requirement range for sample completion, thus establishing flexibility. Furthermore, inspection resources have been adjusted in the security baseline inspection program to reallocate resources to areas, as identified by regional inspectors, requiring additional oversight.

Champion and Key Branch Chief: Ron J. Albert, NSIR/DSO
Key Staff: Scot Sullivan, NSIR/DSO

In addition, adjustments to the security baseline procedures have been completed to eliminate redundancies in the inspection program. In the area of cyber security, the Cyber Security Directorate is developing guidance to reduce engineering judgment related to cyber security inspections. Lastly, with regards to openness after September 11, 2001, the Commission moved to strike security inspection reports from the public purview, to ensure that the information would and could not be used by an adversarial force. The U.S. Nuclear Regulatory Commission is fully committed to its goal of ensuring openness in its regulatory process, but must balance that goal with ensuring the continued safety and secure operation of nuclear facilities.