SECURITY ISSUES FORUM CHARTER

1.0 Background

As a result of the terrorist attacks, on September 11, 2001, the U.S. Nuclear Regulatory Commission (NRC) issued Orders and Confirmatory Action Letters to licensees containing enhanced security requirements. The regulatory framework to incorporate the measures was developed and is currently in place. To ensure the consistent application and resolution of inspection findings, the Compensatory Measures Management Review Panel (CMMRP) was created on September 11, 2003.

Further, to ensure regulatory consistency for all security-related discoveries and violations, including regulatory requirements in Title 10 of the *Code of Federal Regulations*, the CMMRP charter was updated to reflect the CMMRP's role of reviewing all regional and headquarters findings. Then, on April 1, 2005, the CMMRP changed its name to the Security Findings Review Panel (SFRP), to reflect the status of the panel's efforts.

Subsequently, the Security Issues Forum (SIF) replaced the SFRP on August 31, 2009, to provide an environment for the discussion of security findings, violations, and other issues of common interest upon request. In addition to potential findings or violations, all communications that were previously processed through the Report on Interactions process will now be submitted to the SIF, using the forms [*SIF Worksheet (Template)* and *SIF Interaction Document*] for discussion and disposition.

2.0 Purpose

The SIF provides a forum for regional and headquarters staff to solicit input from each other regarding security inspection-related questions, first-time security findings/violations, self-revealed findings, target set findings, and other security issues. The SIF may also present an opportunity to discuss Operating Experience (OpE), industry trends, and other relevant security Items of concern. Information shared in the SIF is provided for participants' awareness and consistency purposes.

3.0 Scope

- All inspection findings and violations, including 1) target set findings, 2) self-revealed findings, and 3) first-time security findings, related to any new security requirements that are not of an established routine nature or are on the SIF SharePoint site, should be sent to the Security Oversight and Support (SOSB) Branch Chief and the SIF coordinator for review and assessment by close of business the Friday preceding the Wednesday SIF.

- The SIF is scheduled for every Wednesday or as needed. SIF participants will review and discuss security inspection-related questions, first-time security findings/violations, target set findings, self-revealed findings, and other security issues, as requested by regional and headquarters staff.

- Wrongdoing findings or violations that are part of an ongoing investigation by the Office of Investigation will not be paneled by the SIF until the outcome of the investigation is finalized by the NRC.

- The SIF SharePoint site will identify all findings and violations that have been reviewed by the SIF participants, including examples of minor findings. Participants are encouraged to review the SIF SharePoint site and Operating Experience (OpE) SharePoint site before submitting the SIF worksheet for panel discussions.

3.1 Roles and Responsibilities

The SIF coordinator will:
(a) collect all items for discussion, based on the requested topics submitted by the staff;
(b) distribute the Agenda and SIF worksheets for the meetings;
(c) facilitate the weekly meetings; and
(d) collect and maintain all SIF worksheets in the SharePoint database.

Presenters shall provide the SIF coordinator with a completed *SIF Worksheet (Template)* specifying the purpose and a concise description of the issue to be discussed at the SIF. This to the SIF coordinator, for dissemination to SIF participants. If the contents of the SIF worksheet contain Safeguard Information (SGI), then the information must be transmitted using the Safeguards Information Local Area Network and Electronic Safe. SIF worksheets that are unclassified or SGI will be disseminated to all SIF participants by the SIF coordinator.

If the contents of the SIF worksheet contain CLASSIFIED information, then the information must be delivered, in accordance with the appropriate requirements for the transmission of CLASSIFIED information. It is the responsibility of the originating office to disseminate SIF worksheets that contain CLASSIFIED information to staff in the participating regions and offices.

3.2 Participation

Primary participants of the SIF should consist of designated representatives from NSIR, the Office of Enforcement, the Office of the General Counsel, and the four Regional Offices. Other NRC offices, such as Office of Nuclear Reactor Regulation and the Office of Nuclear Material Safety and Safeguards, will be included, depending on the issues discussed, as shown in the following table. NSIR will ensure participation by the appropriate specialists, knowledgeable on the issues, presented at the SIF. The senior representative from NSIR serves as the SIF Chair.

Branch Chief or Designee	Role
NSIR DSO/SOSB Branch Chief or Designee	Chair
NSIR DSO/SPEB Branch Chief or Designee	Participant
NSIR DPCP/RSB Branch Chief or Designee	Participant
NMSS Branch Chief or Designee	Participant
NRR Branch Chief or Designee	Participant
OGC Branch Chief or Designee	Participant
OE Branch Chief or Designee	Participant
Region I Branch Chief or Designee	Participant
Region II Branch Chief or Designee	Participant
Region III Branch Chief or Designee	Participant
Region IV Branch Chief or Designee	Participant

Following the guidance in Inspection Manual Chapter 0609, Attachment 5, Inspection Finding Review Board (IFRB), the SIF will be modified to discuss inspection findings that involve complexities such that the outcome of the Significance Determination Process (SDP) is unclear and/or potentially greater than Green determination. Further, the modified SIF must include a Senior Executive Service manager/sponsor for the findings to ensure IFRB processes are being met. However, a modified SIF is not necessary when the significance of the finding, using SDP flowcharts, appears to be clear and straightforward, regardless of proposed significance.

3.3 Consensus

While no votes will be taken on findings or violations that are discussed, a consensus of the appropriate course of action should be obtained from the participating SIF members. Areas of disagreement should be raised through normal Division-level management channels to gain resolution.

3.4 Level of Effort

Participation and level of effort is dependent upon the complexity of the issues.

4.0 Glossary of Terms

First-Time Findings
Findings that the security program has not established a precedence (no record exist that we have dispositioned this type of finding) and/or the finding is being dispositioned differently than previous findings (i.e., different requirement cited).

Self-Revealed Findings
Self-revealed findings or violations are those identified as a result of a condition that (1) become apparent through a readily detectable degradation in material condition, capability, or functionality of equipment or plant operations; and (2) does not meet the definition of licensee-identified or NRC-identified.

Target Set related Findings
Findings related to the development, identification, and maintenance of target sets.