CHARTER FOR THE INFORMATION SECURITY STEERING COMMITTEE

November 16, 2009

Information security at the U.S. Nuclear Regulatory Commission (NRC) is a critical component of achieving the NRC's overall mission and includes the appropriate use of all information owned, regulated or under the control of the NRC, in all of its forms, by both internal and external entities. This includes the protection of information through physical security, personnel security, and cyber security efforts, as well as security of intelligence information. The key challenge associated with implementing an effective NRC-wide information security program is to establish a balance between ensuring that information is readily available when needed, while protecting the information (and associated information systems) from unauthorized access, use, disclosure, disruption, modification, or destruction.

Achieving this balance and establishing an NRC-wide information security program is made more complex by the number of entities involved in the protection of information, and the nature of their responsibilities. Additionally, as previously separated functions merge and mechanical controls are digitized, the vulnerability of critical operational data and operations is increased and the threat is intensified. Consequently, the appropriate use of information security controls to ensure the security of nuclear materials and reactors is of particular importance to the NRC's regulatory efforts.

On November 14, 2007, the Commission directed the staff to develop a comprehensive information security strategy (reference SRM-S07-0181). The NRC Deputy Executive Director for Corporate Management and Chief Information Officer (DEDCM/CIO) subsequently determined that this comprehensive strategy should take the form of an Information Security Strategic Plan (ISSP), and should be guided by an Information Security Steering Committee (ISSC), which was formally chartered on August 12, 2008. On May 21, 2009, the Executive Director for Operations (EDO) provided the Commission the draft ISSP (reference SECY-09-0077) to provide high-level direction and prioritization of agency information security activities. The draft ISSP was also made available for public comment in a Federal Register Notice at that time, however there were no comments received from the public. Consistent with what the staff described in the Commission Paper, the ISSP is now considered a final document.

The staff conducts a wide range of information security-related activities in practically every NRC office and region. The ISSC purpose is to serve as the NRC's inter-organizational body to conduct information security strategic planning and to perform information security program oversight by providing advice to the EDO and the Deputy EDOs. The Steering Committee also supports line managers engaged in the implementation of the agency information security strategic plan by assisting in the resolution of policy or programmatic issues affecting multiple offices.

1 ISSC PURPOSE

The ISSC, comprised of senior executives of selected major NRC offices having information security responsibilities, provides strategic direction to the staff in implementation and maintenance of the NRC ISSP. The ISSC functions under the authority of the EDO and provides advice to the EDO and the Deputy EDOs in NRC information security matters.

2 ISSC MEMBERSHIP

The ISSC membership will be from the following offices assigned at the discretion of the responsible office director:

- Computer Security Office
- Office of Administration
- Office of Federal and State Materials and Environment Management Programs
- Office of Information Services
- Office of New Reactors
- Office of Nuclear Material Safety and Safeguards
- Office of Nuclear Reactor Regulation
- Office of Nuclear Regulatory Research
- Office of Nuclear Security and Incident Response
- Regional Offices (one representative agreed upon by the four regions)

Members are charged with representing the interests of the agency as a whole rather than those of their sponsoring offices. Members representing the Computer Security Office (CSO) and the Office of Nuclear Security and Incident Response (NSIR) serve as ISSC co-chairs, and administrative support for the ISSC is provided by the offices of the co-chairs.

3 ISSC APPROACH

ISSC decisions or recommendations to senior management are made based upon the consensus of the membership. The ISSC advises the offices and provides an inter-office coordinating function for the implementation of the ISSP. The ISSC may recommend the formation of working groups, consistent with office budgets and resource availability, to coordinate/facilitate development of important guidance documents or work out important interoffice information security-related issues.

The ISSC will meet at least quarterly to review progress in ISSP implementation, to review and guide the activities of established working groups, and to recommend to the offices where changes in approach are necessary. The ISSC reviews products produced by the working groups and recommends their approval. The ISSC conducts a formal triennial review of the ISSP and updates the plan as necessary to ensure it remains current.

4 ISSC RESPONSIBILITIES

To achieve its stated purpose, the ISSC:

- Monitors the implementation of the NRC information security strategic plan to include making recommendations to the offices on prioritization of efforts, as appropriate. This should include supporting the inclusion of necessary resources through the planning and budgeting process.

- Maintains awareness of the activities of the Cyber Assessment Team (CAT) relative to its response to emergent cyber security incidents that potentially affect NRC regulated facilities, and provide support to the CAT in disposition of issues as requested.

- Provides to the EDO annually a formal report on the status of the NRC information security program.

- Formally reviews and updates the ISSP every three years.