

CHARTER FOR INFORMATION SYSTEM SECURITY OFFICER FORUM

July 14, 2009

On March 30, 2009, the Executive Director for Operations directed the Computer Security Office (CSO) to establish the Information System Security Officer (ISSO) Forum to provide a communication mechanism for computer security information between the Computer Security Office (CSO), the Chief Information Security Officer (CISO), and the ISSOs as well as among ISSOs. The ISSO Forum is a key component of the U.S. Nuclear Regulatory Commission (NRC) -wide Computer Security Program, and serves as a communication mechanism for the CSO in their management of the program. The ISSO Forum is chaired by the CISO or his designee.

1 BACKGROUND

Information security at the 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 computer 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 computer 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 computer security controls to ensure the security of nuclear materials and reactors is of particular importance to the NRC's regulatory efforts.

2 ISSO FORUM PURPOSE

The purpose of the ISSO Forum is to provide a communication mechanism for CSO staff and ISSOs to communicate, collaborate, and exchange information relevant to the NRC computer security program. Under CSO leadership, the forum will focus on the dynamic Information Technology (IT), business, and operational environments and their influence over risks, costs, strategies, policies, and solutions. The ISSO Forum will be advisory to the CSO/CISO.

3 ISSO FORUM VISION

NRC ISSOs provide organizational information that enables the CSO to implement an NRC computer security program that appropriately balances computer security with business needs, and NRC ISSOs increase their computer security knowledge, skills, and abilities.

4 ISSO FORUM APPROACH

The ISSO Forum will conduct monthly meetings to enable the exchange of computer security knowledge and ideas, upcoming issues of importance to the CSO and ISSOs, and training opportunities. To facilitate consistent and effective communications, the ISSO Forum will employ various mechanisms that will include the CSO webpage and a group email address. The forum will not be used as a venue to discuss implementation issues, however, an OIS

senior manager will be present at the meetings to acquire an awareness of implementation issues that impact computer security. Proposed agenda items from the membership are sent to the ISSO forum executive secretary at least one week prior to the meeting.

5 ISSO FORUM MEMBERSHIP

The ISSO Forum consists of NRC staff assigned duties as primary and alternate office ISSOs by office directors and regional administrators. Each office has a single membership except for the Office of Nuclear Security and Incident Response (NSIR), Division of Security Operations, Information Security Branch. This branch appoints an ISSO primary and alternate in addition to the primary and alternate appointed by the NSIR office director due to their unique security role within the NRC. Those offices deemed too small to have an individual ISSO may band together to appoint a single Office ISSO and alternate as their membership in the forum. The CSO Senior IT Security Officers (SITSOs) are members and they or their designee provides computer security information at each monthly forum. The CISO chairs the ISSO forum and an office ISSO is elected as co-chair for a one-year term. Each member has a vote.

The ISSO member should attend each forum meeting. Members ensure that other ISSOs within their offices receive the information communicated via this forum.

6 ISSO FORUM OBJECTIVES

The ISSO Forum has the following objectives:

- Provide a vehicle for CSO to inform ISSOs of critical IT security information
- Provide a mechanism for interchange of computer security knowledge and skills;
- Establish and maintain relationships between individual ISSOs and the CSO staff to facilitate actively addressing information system security issues within the NRC;
- Establish and maintain a comprehensive, proactive approach to identifying and resolving programmatic and tactical information system security issues involved in the development and application of new and emerging computer security solutions, and;
- Assist CSO in developing security policies by providing implementation impacts.

7 MEMBERSHIP VOTING

The ISSO forum membership votes anonymously on the following:

- ISSO forum co-chair appointment annually or upon co-chair resignation
- Computer security recommendations to the CSO
- Working group establishment

8 ISSO FORUM WORKING GROUPS AND THEIR MEMBERSHIP

As deemed necessary by the ISSO Forum, working groups may be formed to address specific computer security topics. The purpose, scope, and membership will be determined at the time a working group is established.

9 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities associated with the ISSO forum.

9.1 Chief Information Security Officer

The CISO serves as the Chair of the ISSO Forum. The Chair provides vision, leadership, direction, and oversight of the ISSO Forum. The Chair provides guidance in addressing issues of importance to the CSO and Office ISSOs. The Chair casts the tie breaking vote on all ISSO Forum issues.

9.2 ISSO Forum Co-Chair

The ISSO Forum co-chair serves as the primary point of contact between CSO and the other office ISSOs. Members may identify topics of consideration for the forum or may provide forum suggestions through the co-chair. The co-chair proposes forum agenda topics to the executive secretary.

9.3 CSO Policy, Standards and Training (PST) SITSO

The CSO PST SITSO attends or designates an attendee for the monthly ISSO Forum meetings and serves as the chair designate (assumes leadership of the Forum if the Chair is unavailable.) The CSO PST SITSO provides updates on CSO policy, standards, and training; ensures appointment of the forum executive secretary from his/her staff, and facilitates the ISSO Forum.

9.4 CSO FISMA Compliance and Oversight (FCO) SITSO

The CSO FCO SITSO attends or designates an attendee for the monthly ISSO Forum meetings and provides updates on FISMA compliance, such as system C&A efforts and plans of action and milestones.

9.5 CSO Computer Situational Awareness, Analysis & Response (CSAAR) SITSO

The CSO CSAAR SITSO attends or designates an attendee for the monthly ISSO Forum meetings and communicates computer security situational awareness information such as security alerts, advisories, and bulletins.

9.6 ISSO Forum Executive Secretary

The ISSO forum executive secretary is the CSO point of contact for forum members and performs the following functions:

- Arranges for meeting dates, space, and necessary conferencing services
- Develops meeting agendas
- Documents meeting minutes
- Tallies anonymous votes
- Compiles input received from the membership and provides the input to CSO
- Emails information to the membership

9.7 Office ISSO

The Office ISSO attends or designates an attendee for the monthly ISSO Forum meetings. The Office ISSO functions as the distribution point for appropriate information back to other ISSOs

within their office and where appropriate to all office staff. Only those formally appointed as the Office ISSO will have a vote on Forum issues. Only one vote may be cast per office. For those Office ISSOs that are representing a group of smaller offices, only one vote may be cast for that group. The Office ISSO serves as the principal point of contact for their office's system ISSOs. In turn, the Office ISSO will bring forward items of concern to their system ISSOs for consideration by entire Forum.