March 30, 3009

MEMORANDUM TO: Those on the Attached List

FROM: Patrick D. Howard, Director ***/RA/***
Computer Security Office

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION INFORMATION SYSTEM SECURITY OFFICER FORUM

The Information System Security Officer (ISSO) Forum is being established under the authority of the Executive Director for Operations to provide a communication mechanism for computer security information between the Computer Security Office (CSO) and the ISSOs as well as among ISSOs. The ISSO Forum will be a conduit for CSO staff and ISSOs to regularly collaborate and exchange computer security materials and knowledge. The ISSO Forum will be chaired by the Chief Information Security Officer or his designee.

This memorandum is to request your support and action for the ISSO Forum. As office directors and regional administrators, you will need to appoint a single ISSO and alternate to serve as liaison to this forum and ensure that other office ISSOs receive the information communicated via this forum.

I have enclosed an ISSO Forum concept paper for your review and feedback. The CSO is requesting your feedback no later than April 27, 2009. I appreciate your assistance in this matter.

CONTACT: Kathy Lyons-Burke, CSO/PSTT
301-415-6595

Enclosure:
As stated

March 30, 2009

MEMORANDUM TO: Those on the Attached List

FROM: Patrick D. Howard, Director ***/RA/***
Chief Information Security Officer

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION INFORMATION SYSTEM SECURITY OFFICER FORUM

The Information System Security Officer (ISSO) Forum is being established under the authority of the Executive Director for Operations to provide a communication mechanism for computer security information between the Computer Security Office (CSO) and the ISSOs as well as among ISSOs. The ISSO Forum will be a conduit for CSO staff and ISSOs to regularly collaborate and exchange computer security materials and knowledge. The ISSO Forum will be chaired by the Chief Information Security Officer or his designee.

This memorandum is to request your support and action for the ISSO Forum. As office directors and regional administrators, you will need to appoint a single ISSO and alternate to serve as liaison to this forum and ensure that other office ISSOs receive the information communicated via this forum.

I have enclosed an ISSO Forum concept paper for your review and feedback. The CSO is requesting your feedback no later than April 27, 2009. I appreciate your assistance in this matter.

CONTACT: Kathy Lyons-Burke, CSO
301-415-6595

Enclosure:
As stated

DISTRIBUTION: See next page

ADAMS Accession No.: ML090840313

OFFICE:	CSO/PSTT	CSO/PSTT	CSO
NAME:	R. Hardy	K. Lyons-Burke	P. Howard
DATE:	03/26/09	03/27/09	03/30/09

OFFICIAL RECORD COPY

MEMORANDUM TO THOSE ON THE ATTACHED LIST DATED: March 30, 2009

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION INFORMATION SYSTEM SECURITY OFFICER FORUM

Edwin M. Hackett, Executive Director, Advisory Committee on Reactor Safeguards	T-2 E26
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and Licensing Board Panel	T-3 F23
Karen D. Cyr, General Counsel	O-15 D21
Brooke D. Poole, Acting Director, Office of Commission Appellate Adjudication	O-16 G4
James E. Dyer, Chief Financial Officer	T-9 F4
Hubert T. Bell, Inspector General	O-5 E13
Margaret M. Doane, Director, Office of International Programs	O-4 E21
Rebecca L. Schmidt, Director, Office of Congressional Affairs	O-14 F2
Eliot B. Brenner, Director, Office of Public Affairs	O-16 D3
Annette Vietti-Cook, Secretary of the Commission	O-16 G4
R. William Borchardt, Executive Director for Operations	O-16 E15
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research, State, Tribal, and Compliance Programs, OEDO	O-16 E15
Darren B. Ash, Deputy Executive Director for Corporate Management, OEDO	O-16 E15
Bruce S. Mallett, Deputy Executive Director for Reactor and Preparedness Programs, OEDO	O-16 E15
Vonna L. Ordaz, Assistant for Operations, OEDO	O-16 E15
Timothy F. Hagan, Director, Office of Administration	TWB-5 E19M
Patrick D. Howard, Director, Computer Security Office	T-2 C2M
Cynthia A. Carpenter, Director, Office of Enforcement	O-4 A15a
Charles L. Miller, Director, Office of Federal and State Materials and Environmental Management Programs	T-8 D22
Guy P. Caputo, Director, Office of Investigations	O-3 F1
Thomas M. Boyce, Director, Office of Information Services	O-6 E07
James F. McDermott, Director, Office of Human Resources	GW W5A6
Michael R. Johnson, Director, Office of New Reactors	T-6 F13
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards	EBB 1
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation	O-13 D13
Brian W. Sheron, Director, Office of Nuclear Regulatory Research	C-6 D20M
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights	O-3 H8
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response	T-4 D22A
Samuel J. Collins, Regional Administrator, Region I	RI
Luis A. Reyes, Regional Administrator, Region II	RII
Mark A. Satorius, Regional Administrator, Region III	RIII
Elmo E. Collins, Jr., Regional Administrator, Region IV	RIV

U.S. Nuclear Regulatory Commission Information System Security Officer Forum

Purpose

The Information System Security Officer (ISSO) Forum is being established under the authority of the Executive Director for Operations to provide a communication mechanism for computer security information between the Computer Security Office (CSO) and the ISSOs as well as among ISSOs. The ISSO Forum will be a conduit for CSO staff and ISSOs to regularly collaborate and exchange information security materials and knowledge. The ISSO Forum will be chaired by the Chief Information Security Officer (CISO) or his designee.

Authority

The authority of the ISSO Forum will be established by means of a memorandum issued by the Executive Director for Operations.

Objectives

The ISSO Forum has the following objectives:

- Provide a vehicle for CSO to inform ISSOs of critical Information Technology (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 U.S. Nuclear Regulatory Commission (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 information security solutions, and;
- Assist CSO in developing security policies by providing implementation impacts.

ISSO Forum Membership

The ISSO Forum will consist of individuals assigned duties as ISSO for general support systems and major applications. The identification should be sent to the Senior IT Security Officer for policy, standards, and training by May 1, 2009. Either the primary or alternate ISSO must attend each forum meeting. Representatives of other offices may attend forum meetings but will not be permitted to vote as members of the forum.

The following information is needed for each forum member:

Primary ISSO Name:
Office/Region:
Contact Information
Location: Mailing address, mail stop
Primary phone number:
Alternate phone number:
Email Address:

Alternate ISSO Name:
Office/Region:
Contact Information
Location: Mailing address, mail stop
Primary phone number:
Alternate phone number:
Email Address:

ISSO Forum Charter

The members of the ISSO Forum will develop a charter which at a minimum will address the following:

- Purpose
- Objectives
- Approach
- ISSO Forum membership
- ISSO Forum working groups and their membership
- ISSO roles and responsibilities

Meeting Schedule

The ISSO forum will meet every two months for approximately 1 hour, until the need for a different schedule is established. The first meeting will take place on: June 1, 2009.

The ISSO meeting agenda will be sent to all ISSO forum members at least 3 days prior to the scheduled meeting. ISSOs are welcome to submit proposed agenda items. Meeting minutes will be recorded and distributed to all ISSO forum members within 5 business days.

ISSO Forum Communications

To facilitate consistent and effective communications, the ISSO Forum will employ various mechanisms that will include the CSO webpage and a group email address.

Initial Meeting Agenda

- Forum Participant Role call
- Opening remarks - CISO
- ISSO Forum Overview
  - Purpose
  - Objectives
- Computer Security Program
  - Computer security policy update
  - Computer security standards and guidance update
  - Computer security training update
  - Federal Information Security Management Act compliance

process/procedure update
- Situational awareness/incident response update

- Questions/Comments
- Action Item Review

System ISSO - Level Roles/Responsibilities:

The ISSO serves as the principal point of contact for all IT security aspects of an IT system. The ISSO also manages the security aspects of the information system and daily security operations (e.g., data security, physical and environmental security, personnel security, incident handling, enterprise continuity, regulatory and standards compliance, and security awareness and training). He/she works with system owners to document weaknesses in Plans of Action and Milestones and to oversee corrective action. In addition, he/she assists in the development of the system security documentation, ensures compliance with the NRC IT security policy on a routine basis, and monitors effectiveness of system security controls.

The ISSO is expected to have a technical understanding of computer operations as well as the technical knowledge, skills, and abilities necessary to ensure the security for the system for which he/she is responsible. Annual computer security awareness training is required for each ISSO and completion of each of the following every 3 years:

- ISSO role specific training (not awareness) provided by a government agency or by an organization such as SANS or $(ISC)^2$
- Vendor specific operating system security control training (e.g., Windows, Unix/Linux)
- Vendor specific application security training (e.g., Oracle, Java, WEB Apps, .NET)

The ISSO must have a clearance and background investigation appropriate for the highest security level of information processed by the IT system. The ISSO is responsible for implementing the requirements of Management Directive 12.5 and any other system-specific security activities. Specific ISSOs responsibilities include the following:

- Developing (or assisting in the development of) the security rules of behavior specific to the office-sponsored IT systems.
- Monitoring compliance with the IT system security rules of behavior and other security controls.
- Ensuring users and system support personnel have required security clearances, authorization and need-to-know, are indoctrinated, and are familiar with internal security practices before access to the IT system is granted. Periodically review the personnel security program for compliance with standards, procedures, directives, policies, regulations and statutes.
- Maintaining a plan for site security improvements and progress towards meeting accreditation to ensure that the IT system certification and accreditation process is completed before systems are placed into operation. The ISSO will coordinate for the system owner with CSO for any assistance required to support system security accreditation.

- Ensuring that IT system security program reviews and annual security controls testing and contingency plan testing are completed, as well as, initiating protective or corrective measures as needed.
- Ensuring that the status of remediation activities is tracked and reported until successfully completed.
- Responding to, investigating, and reporting security incidents to the Computer Incident Response Team (CIRT), 301-415-6666 or CS_IRT@nrc.gov.
- Performing periodic reviews of system audit trails and access control lists.