CHARTER FOR INFORMATION SECURITY STEERING COMMITTEE AND WORKING GROUPS
October 15, 2008

Information security at the 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). In addition, on March 18, 2008, the NRC’s Office of the Inspector General (OIG) issued a Memorandum Report entitled, “NRC’s Planned Cyber Security Program (OIG-08-A-06),” that assessed how upcoming changes to NRC’s cyber security oversight processes might impact the agency’s physical security inspection program. In this report, the OIG identified the issue that the NRC has not finalized a clear plan for implementation of a cyber security inspection program.

The staff is currently conducting a wide range of information security-related activities in nearly all NRC offices and regions. The formation of an Information Security Steering Committee (ISSC) will enable NRC to fulfill both its strategic planning responsibilities and its information security issue resolution responsibilities by providing advice to the Deputy Executive Director for Reactor and Preparedness Programs and the DEDCM/CIO. This Steering Committee will also support line managers who are accountable for the implementation of NRC’s information security responsibilities. The ISSC through its working groups will be available to address information security issues that arise related to NRC’s regulatory responsibilities, inclusive of cyber security, by gathering together those staff members who possess the necessary skills to address all aspects of the issues. The ISSP development effort will result in a proposal for the effective performance of information security activities across the NRC, provide the NRC with a clear information security vision, and align the NRC’s information security activities to attaining that vision.
1 ISSC PURPOSE
The ISSC, comprised of senior managers from each major NRC office with information security responsibilities, will provide strategic direction to the staff in development and implementation of the NRC information security program. Two immediate projects have been selected: 1) development of an NRC information security strategic plan and 2) development of a viable approach to address cyber security incidents that occur at licensee organizations.

2 ISSC MEMBERSHIP
The initial ISSC membership will be as follows allowing that new members will be selected at the discretion of responsible management.

Darren Ash, EDO
Sher Bahdur, NRR
Anne Boland, Region III
Tom Boyce, OIS
Bill Dean, NSIR
Dan Dorman, NMSS
Farouk Eltawila, RES
Jennifer Golden, FSME
Thorne Graham, CSO
Barbara Gusack, NRO
Ray Hardy, CSO
Pat Hiland, NRR

Patrick Howard, CSO
Art Howell, Region IV
Chris Hoxie, RES
Kathy Lyons-Burke, CSO
Bruce Mallett, EDO
Scott Morris, NSIR
Trip Rothschild, OGC
Rick Rough, OCFO
James Schaeffer, OIS
Connie Schum, NRO
Bob Webber, ADM

3 ISSC APPROACH
The ISSC will use 2 working groups; one to develop an NRC information security strategic plan and one to develop a viable approach to address cyber security incidents that occur at licensee organizations. The ISSC will meet at least monthly to obtain progress reports from established working groups and guide their efforts. The ISSC will review and provide final approval on the products produced by the working groups. Depending upon the results of the working group efforts, one or more steering committees may be established on an on-going basis to oversee and guide efforts in the information security area.

4 ISSC OBJECTIVES
The ISSC will establish and provide strategic direction to two working groups. The ISSC will:

1. Ensure development of a comprehensive NRC information security strategic plan
2. Ensure development of an approach for NRC to respond to emergent information security issues related to NRC’s regulatory responsibilities

5 INFORMATION SECURITY STRATEGIC PLAN WORKING GROUP
The ISSP Working Group (WG) is established to develop a comprehensive NRC information security strategic plan. The plan will provide information regarding NRC’s current information security efforts and will propose a strategy to achieve all information security responsibilities that are part of the NRC mission.
5.1 ISSP WG Membership
The initial ISSP WG membership will be as follows allowing that new members will be selected at the discretion of responsible management.

Kathy, Lyons-Burke, CSO – Lead
Scott, Morris, NSIR – Lead
Elizabeth Chew, OIS/ICOD
Ralph Costello, NSIR
David Ditto, NMSS
Craig Erlanger, NSIR
Harry Felsher, FSME
David Furst, NSIR
Russell Gibbs, NRR
Cameron Goodwin, NRR
Teresa Grancomvit, RES
Gerald Gulla, OE
Ray Hardy, CSO
Wesley Held, NRO
Nick Hilton, OE
Linda Howell, Regions
Skip Kemerer, OIS/BPIAD
Russell Nichols, OIS/IRSD
David Offutt, OIS/ICOD
Andrew, Pretzello, ADM
William Reckley, NRO
David Rahn, RES
Sandy Schoenmann, ADM
Lynn Silvious, NSIR
Brian Smith, NMSS
Karl Sturzebecher, RES
Bobbi Warren, NSIR
Garmin West, NSIR

5.2 ISSP WG Approach
The ISSP WG will work with NRC staff to develop a comprehensive NRC information security strategic plan. The strategic plan will follow the same basic format that is followed by the Information Technology/Information Management strategic plan.

5.3 ISSP WG Objectives
The ISSP will:

1. Identify all current information security efforts and responsibilities, including those associated with security policy and guidance development, rulemaking, licensing, oversight, inspection, and enforcement
2. Identify the lead and supporting offices currently managing and performing the information security work
3. Identify the total scope of information security efforts NRC should be performing, specifically stating the current gaps
4. Inventory existing human capital and financial resources allocated to information security in the Fiscal Year (FY) 2009 approved budgets across all affected offices/regions
5. Identify a proposed mapping of the information security responsibilities for the desired scope
6. Determine any additional resources needed to address any shortcomings identified in the above-directed analyses
7. Establish priorities and time tables for implementing all required actions
8. Develop other action plans and monitoring processes (where applicable)
9. Deliver the ISSP incorporating the information obtained through above-directed analyses
6 LICENSEE SECURITY INCIDENT RESPONSE WORKING GROUP

The Licensee Security Incident Response (LSIR) WG is established to develop an approach for NRC to respond to emergent information security issues related to NRC’s regulatory responsibilities. The approach will provide a detailed process, including required resources, to respond to the cyber issues.

6.1 LSIR WG Membership

The initial LSIR WG membership will be as follows allowing that new members will be selected at the discretion of responsible management.

George Wilson, NRR – Lead
Nitin Patel, NRR
Karl Sturzebecher, RES
John Pellet, Region IV
James McCarthy, CSO
Craig Erlanger, NSIR
David Ditto, NMSS

6.2 LSIR WG Approach

The LSIR WG will work with NRC staff to develop a comprehensive NRC regulatory cyber response plan.

6.3 LSIR WG Objectives

The LSIR will:

1. Analyze and provide recommendations for response to emergent information security issues related to NRC’s regulatory responsibilities, with support from outside expertise (as needed)
2. Identify the lead and supporting offices currently managing and performing the work
3. Identify the total scope of information security efforts NRC should be performing, specifically stating the current gaps
4. Inventory existing human capital and financial resources available in the FY 2009 approved budgets across all affected offices/regions
5. Identify a proposed mapping of the responsibilities for the desired scope
6. Determine what additional resources, if any, are needed to address any shortcomings identified in the above-directed analyses
7. Establish priorities and time tables for implementing all required actions
8. Develop other action plans and monitoring processes (where applicable)
9. Deliver the approach obtained through above-directed analyses
6 LICENSEE SECURITY INCIDENT RESPONSE WORKING GROUP

The Licensee Security Incident Response (LSIR) Working Group (WG) is established to develop an approach for NRC to respond to emergent information security issues related to NRC’s regulatory responsibilities. The approach will provide a detailed process, including required resources, to respond to the cyber issues.

6.1 LSIR WG Membership

The initial LSIR WG membership will be as follows allowing that new members will be selected at the discretion of responsible management.

George Wilson, NRR – Lead
Nitin Patel, NRR
Karl Sturzebecher, RES
John Pellet, Region IV
James McCarthy, CSO
Craig Erlanger, NSIR
David Ditto, NMSS

6.2 LSIR WG Approach

The LSIR WG will work with NRC staff to develop a comprehensive NRC regulatory cyber response plan.

6.3 LSIR WG Objectives

The LSIR will:

1. Analyze and provide recommendations for response to emergent information security issues related to NRC’s regulatory responsibilities, with support from outside expertise (as needed)
2. Identify the lead and supporting offices currently managing and performing the work
3. Identify the total scope of information security efforts NRC should be performing, specifically stating the current gaps
4. Inventory existing human capital and financial resources available in the FY 2009 approved budgets across all affected offices/regions
5. Identify a proposed mapping of the responsibilities for the desired scope
6. Determine what additional resources, if any, are needed to address any shortcomings identified in the above-directed analyses
7. Establish priorities and time tables for implementing all required actions
8. Develop other action plans and monitoring processes (where applicable)
9. Deliver the approach obtained through above-directed analyses