Nuclear Regulatory Commission
Computer Security Office
Standards Working Group Charter

Title:	**CSO Standards Working Group Charter**
Revision Number:	**2.0**
Effective Date:	**September 28, 2012**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary:	The CSO Standards Working Group (SWG) Charter provides the formal written statement of the aims, principles, and procedures of the SWG.
ADAMS Accession No.:	ML12229A305

<table>
<tr><th colspan="5">Approvals</th></tr>
<tr><td><b>Primary Office Owner</b></td><td colspan="2">Policies, Standards, and Training</td><td><b>Signature</b></td><td><b>Date</b></td></tr>
<tr><td><b>Standards Working Group Chair</b></td><td colspan="2">Bill Dabbs</td><td><b>/RA/</b></td><td><b>9/18/12</b></td></tr>
<tr><td><b>Responsible SITSO</b></td><td colspan="2">Kathy Lyons-Burke</td><td><b>/RA/</b></td><td><b>9/19/12</b></td></tr>
<tr><td><b>CSO Standards DAA</b></td><td>CISO</td><td>Tom Rich</td><td><b>/RA/</b></td><td><b>9/18/12</b></td></tr>
<tr><td></td><td>Director, OIS</td><td>Jim Flanagan</td><td><b>/RA/</b></td><td><b>9/19/12</b></td></tr>
</table>

CHARTER FOR THE CSO STANDARDS WORKING GROUP

September 17, 2012

The Information Technology (IT) cyber security standards (also referred to as "cyber security standards") established by the Computer Security Office (CSO) and used throughout the NRC are a key component of the U.S. Nuclear Regulatory Commission (NRC) Cyber Security Program. On July 1, 2011, the Chief Information Security Officer (CISO) established the Standards Working Group (SWG) to provide a consistent mechanism for evaluating, making decisions concerning, and communicating the release of the cyber security standards. The SWG is chaired by the CSO Senior Information Technology Security Officer (SITSO) for Policy, Standards, and Training (PST) or his/her designee.

1 BACKGROUND

Cyber security at the NRC is an essential tool for achieving the NRC's overall mission. The agency cyber security program promotes and supports the appropriate use of all information owned, regulated, or under the control of the NRC, in all of its forms, by internal and external entities. This includes the protection of information through physical security, personnel security, and cyber security efforts.

One challenge associated with implementing an effective NRC-wide cyber security program is establishing a balance between information availability, prevention of unauthorized access, use, disclosure, disruption, modification, or deletion, and the cost of the program. Achieving this balance is complicated due to the number of entities involved in the protection of information, the nature of their responsibilities, and the continuous evolution of IT.

2 SWG PURPOSE

The purpose of the SWG is to evaluate and recommend cyber security standards for use at NRC. The CSO establishes standards to satisfy specific requirements in National Institute of Standards (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; Committee on National Security Systems (CNSS) Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*; Federal Information Processing Standards (FIPS); and the general Office of Management and Budget (OMB), Government Accountability Office (GAO), and NIST 800 SP requirements as appropriate. The CSO also communicates new and updated cyber security standards to NRC Information System Security Officers (ISSOs) and others having cyber security responsibilities.

Cyber security standards establish a common, consistent minimum baseline across the NRC IT Enterprise to minimize the risk to NRC information and IT resources from unauthorized access, use, disclosure, theft, change, deletion, or loss of availability. The standards provide an additional level of protection not afforded by most vendor out-of-the-box default configurations. The objective of the standards is to reduce the number of vulnerabilities that attackers can attempt to exploit, and to reduce the impact of successful attacks.

3 SWG VISION

Cyber security standards are part of the NRC Risk Management Framework and enable the CSO to establish cyber security requirements that are consistent with the business needs and capabilities of the NRC in concert with system development and implementation. The

SWG provides a forum for system owners, developers, and those responsible for implementing standards to discuss the standards as they are developed. The SWG reviews proposed cyber security standards to ensure that they satisfy the intended objective to establish cost effective baseline configurations that provide a reasonable level of security given the threat environment and system categorization.

4 SWG APPROACH

The SWG reviews proposed cyber security standards and makes recommendations concerning the requirements to the CISO. Recommendations may take the form of corrections, additions (if specific requirements have been omitted), and requests to remove specific requirements.

The SWG meets to review current standards, proposed standards, and updates to standards or external standards (from Defense Information Systems Agency (DISA), Center for Internet Security (CIS), or other third party agencies/organizations). Meetings may occur bi-weekly or per another schedule deemed appropriate for the SWG work.

5 SWG PROCESSES

CSO-PROS-3000, “Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards,” provides the process that is used by the SWG to develop, establish, and maintain cyber security standards for information systems that store, transmit, receive, or process NRC information.

The SWG shall determine the order in which development of new standards and revision of existing standards occur using CSO-PROS-3001, “Standards Prioritization Process.”

The initial release and all substantive revisions of CSO-PROS-3000 and CSO-PROS-3001 must be approved by the SWG via the voting process specified in Section 6.2, “SWG VOTING.”

6 SWG COMPOSITION, ROLES, AND RESPONSIBILITIES

6.1 SWG MEMBERSHIP

The following NRC member offices shall be permanent members of the SWG:

1) Computer Security Office (CSO)
    a) CSO representatives shall include the Senior Information Technology Security Officer for PST or his/her designee as the Chair and CSO voting member; SITSO for Cyber Situational Awareness, Analysis, and Response; and the SITSO for FISMA Compliance and Oversight.
2) Office of Information Services (OIS)
    a) OIS shall have one technical representative from the respective cyber security organization in OIS.
3) Regional Offices
    a) The Regional Offices shall be represented by one technical representative. This representative’s role must include cyber security responsibilities of a technical nature. The representative shall be agreed upon collectively by all Regional Offices.

Up to four non-permanent members from the NRC member offices can be selected to participate in the SWG. The members must have recently demonstrated technical cyber security knowledge and experience.

Each member office except CSO shall submit the CSO-TEMP-3000, “Standards Working Group (SWG) Membership Appointment Memo,” to designate a technical representative to participate in the SWG.

The total number of SWG members, to include permanent and non-permanent members, should be between four and seven. Each SWG member may identify an alternate office representative to participate in SWG meetings and activities, which includes voting, if the primary office representative is not available. This alternate must meet the same requirements specified for the primary representative (e.g., must have technical cyber security responsibilities; must be part of a specific organization within the member office).

A complete SWG member listing, including non-permanent member offices, can be found on the CSO web site. The SITSO for PST must approve all changes to NRC member offices and office representatives.

6.2 SWG VOTING

Each SWG member office, whether permanent or non-permanent, shall have only one vote. A population of over half of the SWG member offices is required in order to create a quorum for voting to occur.

A simple majority of votes in favor of a document is required in order for the document to proceed to the ISSO Forum for review and comment. All ISSO forum comments are considered by the SWG, and the SWG shall provide a written comment response to the reviewer. Standards are modified as appropriate based upon review comments. If the standard is modified, a new vote is taken before the standard proceeds to CSO Standards Designated Approving Authority (DAA) approval.

If a tie occurs while voting, then the affected document shall be tabled and set to be voted on for a second time during the next SWG meeting. If a tie occurs during the second time that a document is voted on, the SWG Chair shall cast the tie-breaking vote. The intent of this tie-breaking process is to ensure that the SWG is able to continue to move forward with a clear decision (approval or otherwise) on proposed new and revised documents.

Attendance at meetings may be in person or via teleconference. As situations dictate, documents may be voted on via email. If a vote is taken during a meeting, a voting member must attend in person or via teleconference to vote; if a voting representative cannot attend and misses a vote, that representative may provide an email with his/her stated position on the proposed document after the vote is cast.

Votes are not anonymous, and comments supporting each member office’s vote are encouraged to inform the SWG as to the rationale for support or opposition to a proposed document.

6.2.1 ADMINISTRATIVE CHANGES TO DOCUMENTS

SWG voting and approval is not required for administrative changes to SWG approved documents. Administrative changes include updates to:

- Formatting;
- Grammar;
- Spelling;
- References to other documents (e.g., references to another NRC standard, process, or template; references to external standards);

- Addition of or changes to Uniform Resource Locators (URLs);
- Changes related to updates to external standards, which do not impose additional requirements. Examples of changes related to external standards include the removal of NRC specific requirements, changes in identifiers used to reference requirements in external standards (e.g., DISA Security Technical Implementation Guide (STIG) or CIS identifiers), and the separation of one requirement into two or more requirements; and
- Names and signatures associated with NRC positions when different individuals are appointed to those positions.

6.3 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities associated with the SWG.

6.3.1 SWG CHAIR

The CSO SITSO for PST or his/her designee serves as the SWG Chair and provides vision, leadership, direction, and oversight of the SWG at the direction of the CISO. The SWG Chair appoints the SWG executive secretary from his/her staff, and facilitates the SWG meetings.

The SWG Chair shall review the office membership of the SWG on a periodic basis to adjust non-permanent member offices and/or member office representation, as needed. The SWG chair also ensures appropriate communications with the ISSO forum.

6.3.2 SWG EXECUTIVE SECRETARY

The SWG executive secretary is appointed by the Chair and serves as the PST point of contact for SWG members. He/she performs the following functions:

- Arranges for meeting dates, space, and necessary conferencing services;
- Develops meeting agendas;
- Documents meeting minutes;
- Tallies votes;
- Compiles input received from the membership and provides the input to the Chair; and
- Emails information to SWG members.

6.3.3 SWG MEMBERS

SWG members are responsible for attending bi-weekly meetings, providing input, and voting on recommendations concerning:

- New standards;
- Updates to existing standards;
- Updates to external standards used by NRC standards;
- Effective dates for new or updated standards; and
- Processes and other documents (e.g., the SWG Charter), which support the operations of the SWG.

7 SWG OBJECTIVES

The SWG has the following objectives:

- Provide recommendations for the development of standards;
- Provide a mechanism for communication between office and system ISSOs and the CSO on business and security requirements that impact the development and implementation of standards and impact the operational environment;
- Review, comment, and make recommendations concerning proposed standards; and
- Establish and maintain a comprehensive, collaborative, and proactive process for developing standards involving ISSOs and those responsible for implementing the standards.

8 CHARTER REVIEW AND REVISION

The SWG Charter will be reviewed at least annually. If an update to the SWG Charter is required, the update must be voted on and approved subject to the voting process described in Section 6.2, “SWG VOTING.”

9 SWG CHARTER CHANGE HISTORY

Date	Version	Description of Changes
09-Nov-11	1.0	Initial version
17-Sept-12	2.0	Added information on SWG processes, administrative changes for voting, and clarified roles and responsibilities for the SWG Chair and for SWG members. Removed checklists and guidance to focus the SWG solely on standards. Increased possible non-permanent members to a maximum of four and provided information on an associated request form that must be provided for each non-permanent member. Replaced NSIR as a permanent member with a representative from the Regional Offices.