Nuclear Regulatory Commission
Computer Security Office
CSO Office Instruction

Office Instruction:	**CSO-ADM-0200**
Office Instruction Title:	**Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists**
Revision Number:	**1.0**
Effective Date:	**April 8, 2013**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary of Changes:	CSO-ADM-0200, "Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists," provides guidance regarding format and content of cyber security guidance, procedures, and processes that are developed for NRC staff and contractors across the agency.
Training:	As needed
ADAMS Accession No.:	ML13067A070

Concurrences				
Primary Office Owner	**Policy, Standards, and Training**			
			Signature	Date
Directors	CSO	Thomas Rich	Jon Feibus for **/RA/**	01-Apr-13
	PST	Kathy Lyons-Burke	**/RA/**	01-Apr-13
	FCOT	Paul Ricketts	Ray Hardy for **/RA/**	01-Apr-13
	CSAAR	Thorne Graham	Charles Watkins for **/RA/**	01-Apr-13

Concurrence Meeting Conducted on 01-Apr-13			
Attendees:	Jon Feibus	Kathy Lyons-Burke	Ray Hardy
	Charles Watkins		

CSO Office Instruction
CSO-ADM-0200

Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists

1 PURPOSE

The purpose of CSO-ADM-0200, "Preparing and Maintaining NRC Cyber Security Processes, Procedures, Guidance, Templates, and Checklists," is to provide guidance to CSO staff and managers regarding CSO development of these documents. CSO-ADM-0200 defines a framework for the CSO NRC-level cyber security processes, procedures, guidance, templates, and checklists and defines the process for preparing and maintaining these cyber security aids (CSAs).

Cyber Security Standard development must follow CSO-PROS-3000, "Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards."

2 GENERAL REQUIREMENTS

CSO develops CSAs when CSO management deems CSA development appropriate and necessary. CSAs are intended to facilitate NRC staff and contractor compliance with NRC cyber security requirements.

CSO revises CSAs using the process described in this instruction. Memoranda, e-mails, verbal direction, or other informal communications do not supersede this instruction or CSAs. Line management may, on rare occasions, need to approve a deviation from an established CSA.

Each CSA is managed by the responsible CSO Manager (i.e., Senior IT Security Officer (SITSO) or Chief Information Security Officer (CISO),) and the individual most responsible for the effort is listed as the primary contact. Requests for CSA modification must be approved by the responsible manager.

3 SPECIFIC REQUIREMENTS

The naming convention and corresponding document type for CSAs are provided in Table 1 – CSA Document Naming. For example, the CSA for a cyber security procedure is named CSO-PROC-nnnn, where "nnnn" corresponds to the assigned number for the procedure. The numbering assignments are captured in a spreadsheet maintained by the Policy, Standards, and Training (PST) SITSO and can be found on the CSO G: drive.

Table 1 – CSA Document Naming

Document Naming		Types of Information Contained Within the Document
CKLT	Checklist	A checklist provides a list of items, usually in order of implementation, that helps individuals ensure they covered all required tasks/activities.
GUID	Guidance	Guidance documents provide information on how to use other information, such as a configuration standard.

Table 1 – CSA Document Naming

Document Naming		Types of Information Contained Within the Document
PROC	Procedure	A procedure provides step-by-step detailed instructions to perform a task.
PROS	Process	A process is at a higher level than a procedure and defines a series of steps to accomplish a goal. A process provides more general guidance than a procedure.
STD	Standard	A standard is a specification that must be met.
TEMP	Template	A template provides the structure within which to provide information to CSO, along with the directions on how to fill in the structure.

3.1 Initiating and Preparing Cyber Security Aids

Any CSO staff member or CSO Manager (SITSO or CISO) may suggest a CSA. The suggestion is forwarded to a CSO Manager. The manager decides if the CSA is pursued (if within the responsibility of his or her organization) or may refer the suggestion to another manager. Managers may also decide to pursue a CSA in response to an issue. The responsible manager assigns a primary contact and assists in defining the subject and schedule for developing, reviewing, and issuing the CSA. The CSA primary contact must ensure completed CSAs are placed into ADAMS and posted on the CSO web page.

The primary contact uses the format identified in this instruction (fonts - Arial 11, headers, headings - CSA title and number, etc.) to develop a CSA and includes the contents as summarized in Section 3.2.

3.2 Cyber Security Aid Sections and Content

These sections describe the parts of the CSA.

3.2.1 Cover sheet

The first page of the CSA is a cover sheet that identifies pertinent information about the CSA. Information on the cover sheet includes: CSA identifier, CSA Title, Revision Number, Effective Date, Primary Contact, Responsible Organization, Summary of changes, Training information, the ADAMS Accession Number, the CSO concurrence block, and the table indicating who provided concurrence and when. The cover sheet of this instruction provides a sample of a CSA cover sheet. If a specific concurrence meeting was not conducted and concurrence was performed via email, the concurrence table title is changed to “Concurrence Meeting Conducted via Email and concluded on <Date>”

3.2.2 Purpose

This section provides a brief statement of the purpose of the CSA.

3.2.3 General Requirements

This section provides the higher level guidance and context (e.g., why we have the document), as well as the overarching requirements intended to satisfy specific task requirements, agency policies, and performance goals.

3.2.4 Specific Requirements or Other Appropriate Title

This section provides the basic procedural requirements and guidance (what staff actually need to do). The section explains the requirements as clearly as possible. This may be done by a

step-by-step breakdown, a chronological approach, a flowchart, or other scheme. The main features of the activity or function are described, including but not limited to:

- Initiating an activity (e.g., periodic scan, preparing a security impact assessment)
- Planning for the work
- Executing the plan (conducting the reviews, performing the activity or function, etc.)
- Controlling changes to the plan and reporting changes and progress
- Closing out the activity

3.2.5 Additional Sections as Required

These sections are added where appropriate to convey needed information.

3.2.6 References

If applicable, this section lists key references that an employee must follow in conjunction with use of the CSA, (e.g., Management Directives, OMB Circulars, etc.).

3.2.7 Change History

This section provides a change history table that conveys the date of revision in the format nn-Mmm-yy, the document version, a brief description of the changes made, the method used to announce and distribute the document, and an indication of the training available for the documented activity. The CSO-ADM-0200 change history table is an example.

3.2.8 Appendices

If applicable, appendices can be used for guidance details, templates, or other information that are difficult to confine within the body of the CSA. The format, content, and organization of appendices will depend on the subject of the CSA.

3.3 Cyber Security Aid Review and Approval

The CSA review and approval process consists of three steps:

1. Initial CSO Management review
2. Information System Security Officer (ISSO) Forum review
3. CSO Management review for final approval

3.3.1 Initial CSO Management Review

Each CSA must be provided to the CISO and SITSOs for review and comment. The review period is 2 weeks in duration, but when there is urgency, a 1 week minimum may be applied. Each manager obtains comments from their staff as appropriate. The primary contact must schedule a concurrence meeting at the same time the document is provided for review. The concurrence meeting must occur at the end of the review period. Invited attendees to the concurrence meeting must include all CSO Managers. Each manager may delegate the review meeting as appropriate.

The initial review meeting is conducted and any issues are raised. The attendees at the meeting determine if the document can move to the next phase of the process if the issues are addressed as discussed at the meeting or if another initial review meeting is needed. If another

meeting is required, this phase begins again when the revision is completed. If the document is approved, the CSA primary contact must:

- Record CSO Management concurrence in the document in ADAMS
- Begin the ISSO forum review process

3.3.2 Information System Security Officer (ISSO) Forum Review

After the initial CSO Management review is completed and the determination is made that the CSA is authorized to move to this phase, the CSA must be provided to the ISSO forum for review and comment. The primary contact includes in the email distribution the due date for all comments on the CSA. The review period is 2 weeks in duration, but when there is urgency, a 1 week minimum may be applied. The primary contact collects all comments received from forum members and if necessary, meets with individual members in order to fully understand the comments. The primary contact compiles the comments and proposed responses into a comment/response document and modifies the CSA as appropriate. If no comments are received from the ISSO forum, the primary contact begins the CSA finalization phase.

3.3.3 CSO Management Review for Final Approval

The primary contact provides the revised CSA and comment/response document to the CISO and SITSOs for review and comment. The review period is 2 weeks in duration, but when there is urgency, a 1 week minimum may be applied. The primary contact must schedule a concurrence meeting at the same time the document is provided for review. The concurrence meeting must occur at the end of the review period. Invited attendees to the concurrence meeting must include all CSO Managers. Each manager may delegate the review meeting as appropriate. Each manager obtains comments from their staff as appropriate.

The attendees at the meeting determine if the document can be finalized as is or with minor modifications or if another meeting is required. If the document can be finalized, the primary contact provides the specific responses to those ISSO forum members that provided comments and begins the CSA finalization phase.

If additional work is required, the CISO determines the review phase to which to return the CSA.

3.4 CSA Finalization

All CSAs and significant documents related to CSAs are official agency records. A CSA will be available to the public, unless it contains Sensitive Unclassified Non-safeguards Information (SUNSI). Once a CSA is approved, the primary contact must:

- Record final approval in the document in ADAMS
- Ensure the CSA is posted to the CSO web page on the appropriate page (e.g., procedures must be posted to the CSO procedures web page)
- Request that the document be made into an official agency record
- Provide notification to all CSO staff and all ISSOs regarding the finalization of the CSA

3.5 Maintaining CSO Cyber Security Aids

The primary contact and respective manager are responsible for maintaining the CSA. CSO updates CSAs to reflect changes in organizations; changes in regulations, policies, or

processes; corrections and improvements identified during use of the CSA; and for other reasons that come to the attention of the primary contact or responsible manager.

All CSO staff and managers are expected to identify problems with or possible improvements to CSAs, and to notify the primary contact by e-mail. The primary contact should monitor the use of the CSA by talking with the staff, considering the staff's questions and suggestions, and by occasionally checking documents or other outputs associated with the CSA. The primary contact and responsible manager should, as necessary, initiate minor or major revisions to the CSA.

The primary contact formally reviews the CSA at least annually to ensure that the guidance remains accurate and effective. The review comprises the instruction, a sampling of the associated products, and discussions with or surveys of selected internal (and possibly external) stakeholders. The review shall be documented with an email to the CISO. If the primary contact and responsible manager believe that a CSA no longer serves a useful purpose or that maintaining the CSA is not cost beneficial, the CISO may rescind the CSA. The responsible manager presents the proposal during a routine CSO management meeting and the management team decides whether to retain or rescind the CSA. CSAs, or parts thereof, may also be merged with other CSAs or incorporated into other guidance documents.

3.6 Revising CSO Cyber Security Aids

Revisions to CSAs are classified as either minor or major.

3.6.1 Minor CSA Revisions

Minor revisions have little impact on the allocation of CSO resources and do not change the overall intent of the CSA. CSO staff and managers propose minor revisions to the CSA primary contact to correct identified errors, reflect revisions in other procedures or policies, and incorporate suggested clarifications or improvements. The responsible manager approves minor revisions. The responsible manager describes minor changes to CSAs during routine CSO management meetings. The revision number is incremented by a tenth for the revised CSA. The CSA primary contact follows the process described in section 3.4 to finalize the document after manager approval is obtained.

3.6.2 Major CSA Revisions

Major revisions are changes in policy or procedural matters that warrant office-level approval or that increase or decrease resource estimates by more than one FTE/year. Proposed major changes are discussed during routine CSO management meetings. The primary contact and responsible manager are responsible for major revisions. Major CSA revisions follow the same approval process as a new CSA.

3.7 Cyber Security Aid Training

Primary contacts and responsible managers shall work with other CSO organizations to define and deliver appropriate training for each revision of a CSA. Training may include self-study, meeting presentations, dedicated sessions, and incorporation into qualification programs. In determining the appropriate training strategy, the staff shall consider the importance of the changes to the CSA in terms of meeting legal requirements, the relationship of the procedure to agency policies and performance goals, and how the procedure is used (e.g., frequent or infrequent, general, or specific).

CSO-ADM-0200 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
01-Apr-13	1.0	Pulled agency-wide process out of CSO-ADM-0100	Posting on CSO web page and announcement at CSO biweekly	Upon request