Nuclear Regulatory Commission
Computer Security Office
Computer Security Process

Office Instruction:	CSO-PROS-3001
Office Instruction Title:	Standards Prioritization Process
Revision Number:	1.0
Effective Date:	January 15, 2013
Primary Contacts:	Kathy Lyons-Burke, SITSO
Responsible Organization:	CSO/PST
Summary of Changes:	CSO-PROS-3001, "Standards Prioritization Process," provides the process that is used by the CSO and the Standards Working Group to prioritize the development of new cyber security standards and revision of existing standards.
Training:	As needed
ADAMS Accession No.:	ML12265A326

Approvals				
Primary Office Owner	Policies, Standards, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	11/28/12
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	11/28/12
CSO Standards DAA	CISO	Tom Rich	**/RA/**	12/3/12
	Director, OIS	Jim Flanagan	**/RA/**	12/4/12

TABLE OF CONTENTS

This page intentionally left blank.

Computer Security Process
CSO-PROS-3001

Standards Prioritization Process

---

1 PURPOSE

The CSO establishes cyber security standards to satisfy specific Federal Information Security Management Act (FISMA) requirements and to ensure that information systems (IS) are configured to minimize unauthorized access, use, disclosure, change, deletion, or loss of availability of NRC information. CSO-PROS-3001, "Standards Prioritization Process," is used by the Nuclear Regulatory Commission (NRC) Computer Security Office (CSO) and NRC Standards Working Group (SWG) for prioritizing the development of new cyber security standards and revisions to existing standards.

This prioritization process, together with the SWG Charter and CSO-PROS-3000, "Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards" provides structure to SWG operations as follows:

- The SWG Charter establishes the mission, authority, and rules of the SWG;
- The CSO and SWG prioritize the development of new cyber security standards and revisions to existing standards using CSO-PROS-3001, "Standards Prioritization Process;" and
- The CSO and SWG use CSO-PROS-3000, "Process for Development, Establishment, and Maintenance of NRC Cyber Security Standards" to develop, establish, and maintain cyber security standards for information systems that store, transmit, receive, or process NRC information.

2 GENERAL REQUIREMENTS

NRC cyber security standards are the source of enterprise-wide cyber security requirements and baseline system configurations. Examples include standards that provide organization defined values, password complexity requirements, and baseline system configuration requirements for operating systems, databases, applications (web, client-server, stand-alone), network devices, and mobile devices.

Prioritizing standards development using specific criteria that align with NRC IT enterprise priorities facilitates an impartial ranking of the standards. Towards that end, the SWG is responsible for ensuring that standard evaluation candidates are assessed based on such criteria and in accordance with this process.

Evaluation categories are described in Section 2.1 of this process; the seven step evaluation process and detailed evaluation criteria are provided in Section 3, “Specific Requirements.”

2.1 Evaluation Categories

Evaluation candidates are grouped into the following categories:

1. Enterprise-wide cyber security (e.g., organization defined values, network security, authentication information) and cyber security topics that fall into those areas; and

2. Cyber products and categories of cyber products in use at the NRC (e.g., specific remote access or network access control technologies).

The SWG determines the specific cyber products and categories of cyber products primarily through a review and analysis of the following:

- Technical Reference Model (TRM);
- NRC IT/Information Management (IM) Roadmap and Strategic Plan;
- Current and planned product deployment over the next two years;
- Cyber inventories for NRC information systems and external service providers; and
- Other data sources at the discretion of the SWG.

The SWG is not required to consider products that:

- Have reached or are within one year of their end-of-life for support (or for vendors that do not use end-of-life, 4 years following the initial version release);
- Are scheduled for removal from the production environment within 2 years;
- Are installed or used on less than 100 computing assets; or
- Have not been tied to a mission need.

A sufficient justification must be provided to the SWG for consideration of cyber products with any of the above attributes.

2.2 Evaluation Groups

There are two evaluation groups: new cyber security standards and existing cyber security standards. The overall seven step process described in Section 3.1 applies to both evaluation groups; however, the groups have different prioritization criteria. As part of the seven step process, the SWG must assess evaluation candidates using the prioritization criteria associated with the appropriate evaluation group.

2.2.1 New Cyber Security Standards

The New Cyber Security Standards group consists of new CSO cyber security standards (i.e., standards not currently in existence), and revisions to existing standards that are required to address new technology to be deployed within NRC systems. For example, a revision to an

existing standard driven by the deployment of a new software version, such as an update from VMware ESX Server version 3 to version 4 or 5, would fall within the New Cyber Security Standards group.

The goal for the SWG shall be to spend between 75% and 90% of the SWG's time developing new cyber security standards. The SWG's time is the cumulative number of hours expended on SWG efforts each fiscal year.

2.2.2 Existing Cyber Security Standards

The Existing Cyber Security Standards group consists of revisions to existing CSO standards that are currently effective and published on the CSO Standards web page. This excludes updates to standards that address changes associated with newer technology (e.g., releases of new software versions), as these revisions are considered to be New Cyber Security Standards.

The goal for the SWG shall be to spend between 10% and 25% of the SWG's time revising existing cyber security standards.

3 SPECIFIC REQUIREMENTS

A seven step process has been developed for prioritizing development and maintenance of NRC cyber security standards. Section 3.1 identifies and describes the seven steps. The SWG uses the process to assess each evaluation candidate against specific criteria and obtains an overall score based on the assessment. The relative ranking and priority must be considered separately for evaluation candidates associated with the New Cyber Security Standards and the Existing Cyber Security Standards groups. The final score obtained for each evaluation candidate determines the relative ranking, which is used by the SWG to determine the overall prioritized lists of new standards to be developed and existing standards to be revised each fiscal year.

3.1 Process for Prioritizing Development or Revision of Standards

The seven steps for prioritizing the development and revision of NRC cyber security standards are illustrated in Figure 3-1 and described below. A practical walk-through of the seven step process can be found in APPENDIX D – Seven Step Prioritization Process Walk-Through.

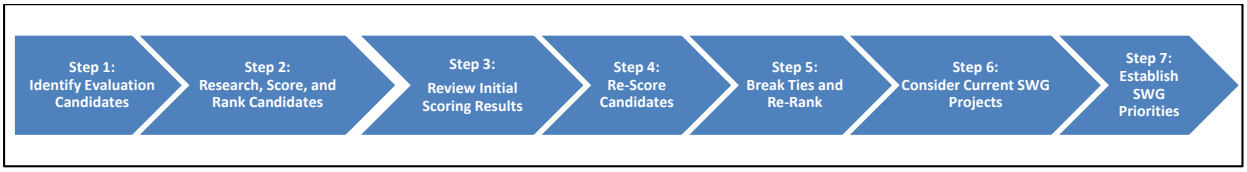

Figure 3-1: Seven Step Prioritization Process

Step 1: Identify Evaluation Candidates

The SWG Chair, or designee, is responsible for enlisting the help of SWG members as well as other NRC program and support offices as needed to identify evaluation candidates.

The SWG must produce a list of evaluation candidates for each evaluation group (specified in Section 2.2).

The SWG must identify any dependencies that exist between evaluation candidates. Dependencies may exist when development of one standard cannot begin until development of another standard is complete or when development of one standard must occur concurrently with development of another standard. An evaluation candidate may have multiple dependencies.

The SWG may, at the discretion of the SWG Chair and with input from SWG members, elect to group multiple closely related evaluation candidates together (e.g., several major versions of a specific software product) as one grouped evaluation candidate). The SWG may only group evaluation candidates that fall within the same evaluation group. For example, the SWG could elect to consider Red Hat Enterprise Linux versions 5 and 6 together. The SWG could also elect to consider multiple endpoint protection technology categories (e.g., anti-malware, host firewall, and host intrusion detection) together.

Step 2: Research, Score, and Rank Candidates

SWG members shall assist the SWG Chair in identifying the evaluation candidates' attribute values (e.g., users or computing assets associated with a specific software product) required to score the candidate. In cases where it is not possible to obtain actual values for all attributes (e.g., due to the lack of an up-to-date count for the number of assets a certain software package is installed on across all NRC information systems), the use of estimates is permitted. Attributes required for prioritization scoring are described in APPENDIX C – Description of Evaluation Candidate Attributes.

The SWG Chair must ensure that each evaluation group is scored using the applicable prioritization criteria. The prioritization criteria are specified in Section 3.2.

If an evaluation candidate (A) has a dependency on at least one other evaluation candidate (B), then the score of the dependent candidate (B) may need to be increased to match that of the evaluation candidate (A). This ensures that the evaluation candidate (A) priority is maintained.

Following scoring, the SWG Chair must ensure that the evaluation candidates within each group are ranked (the highest scoring candidate having the top rank). The result of this step is separate ranking lists for each standards evaluation group containing the rank and score for each evaluation candidate considered.

Step 3: Review Initial Scoring Results

The SWG shall review the results from Step 2. The ranking lists for each evaluation group may include ties where more than one evaluation candidate has the same score.

Based on the ranking identified, the SWG has a second opportunity to group multiple closely related evaluation candidates together (e.g., several major versions of a specific software product) as one grouped evaluation candidate. This method can be used for several purposes, such as resolving ties or changing the score of evaluation candidates through aggregation. Just as in Step 1, the decision to group evaluation candidates

must be done at the discretion of the SWG Chair and with input from SWG members.

If no ties occur and the SWG does not elect to group evaluation candidates together during this step, the SWG shall proceed to Step 6.

Step 4: Re-Score Candidates (if applicable)

For each group of evaluation candidates the SWG elects to group together in Step 3, the SWG must re-score the grouped evaluation candidate.

Step 5: Break Ties and Re-Rank (if applicable)

The intent of the tie-breaking process is to ensure that the SWG is able to continue to move forward with a clear decision on development of new standards and revisions to existing standards.

If there is a tie among at least one of the evaluation candidates (singular or grouped), then the SWG Chair, or designee, shall, with the input of SWG members, determine the relative ranking of the tied evaluation candidates to break the tie.

The SWG shall re-rank evaluation candidates (singular or grouped) in the same manner employed in Step 2.

Step 6: Consider Current SWG Projects

There will likely be SWG projects that are currently being worked that will need to be considered for the next fiscal year prioritization. The SWG shall discuss and recommend, using the subjective factors specified below, to continue, postpone, or stop current SWG projects (e.g., developing new standards, revising existing standards).

- Financial Impact – Impact to budget or opportunity costs (i.e., costs or lost time of forgone product after making a choice)
- Percentage Complete – How close the current effort is to completion, which is based on schedule and time
- Technology Lifecycle – Whether the technology is being phased-out or scaled down in use

For each current SWG project, the SWG Chair, or designee, shall, with the input of SWG members, decide whether to continue, postpone, or stop the project. Projects that are not stopped shall be appropriately considered within the appropriate evaluation group when establishing the SWG priorities for the fiscal year.

Step 7: Establish SWG Priorities

The SWG must review, at a minimum, the following evaluation candidates when establishing SWG priorities for the fiscal year:

- Current work;
- The top 25% of the highest ranked evaluation candidates in the New Cyber Security Standards evaluation group; and

- The top 15% of the highest ranked evaluation candidates in the Existing Cyber Security Standards evaluation group.

The SWG Chair, or designee, shall, through collaboration with SWG members and analysis of historical data, estimate the time required for each evaluation candidate that meets the criteria specified above. This estimated time shall be recorded in the ranking list associated with the candidate.

Based on the SWG's review, the SWG Chair, or designee, shall document the prioritized lists of new standards to be developed and existing standards to be revised for the fiscal year, which is referred to as the "SWG fiscal year (FY) Standards Priorities." Identification of the lists must consider the goals for the expenditure of time by the SWG specified in Section 2.2.

If the SWG opts to conduct the full Standards Prioritization Process more often than the minimum specified frequency in Section 3.3, then the SWG must identify the SWG FY Standards Priorities for, at a minimum, the remainder of the fiscal year.

In order for the standards priorities to proceed to the Designated Approving Authority (DAA) for approval, a quorum of SWG members must vote in majority to do so, subject to the voting requirements specified in the SWG Charter.

Following SWG concurrence, the SWG Chair, or designee, must provide SWG FY Standards Priorities to the CSO Standards DAA for review. The CSO Standards DAA must approve the SWG FY Standards Priorities to enable the SWG Chair to lead, direct, and oversee the operations of the SWG for the fiscal year in accordance with the SWG Charter.

3.2 Prioritization Criteria

The following subsections contain the specific prioritization criteria.

The seven step prioritization process described in Section 3.1 and the prioritization criteria presented in this section must be followed in all circumstances with the following exceptions:

1. A directive from the NRC Chief Information Officer (CIO) automatically moves the evaluation candidate to the top of the priority list or to the priority position directed by the CIO independent of the criteria outlined in this section. This exception takes precedence over the exceptions listed in item 2 below.

2. The following two exceptions automatically move the evaluation candidate to the top of the priority list independent of the criteria outlined in this section; however, these exceptions shall always follow exception 1 in precedence.

   - An external mandate (e.g., from the Office of Management and Budget (OMB)), which is due within 9 months for a specific evaluation candidate.
   - A critical security issue associated with a specific evaluation candidate.

   The SWG Chair shall, with the input of SWG members, use his or her discretion to resolve any conflicts caused when multiple evaluation candidates fall under the above two exceptions.

3. If a directive from the CIO or an external mandate stipulates, directly or indirectly, that the development or revision of a standard; use of a specific software product; or technology category is not permitted or must be postponed for a minimum of two years, then the respective evaluation candidate(s) shall not be considered by the SWG.

Evaluation candidates that fall within the New Cyber Security Standards evaluation group shall be assessed, scored, and ranked using the criteria specified in APPENDIX A – New Standards Prioritization Criteria. Evaluation candidates that fall within the Existing Cyber Security Standards evaluation group shall be assessed, scored, and ranked using the criteria specified in APPENDIX B – Existing Standards Prioritization Criteria.

3.3 Frequency of Standards Prioritization Process Execution

The SWG Chair shall ensure that the SWG executes the Standards Prioritization Process at least once for each fiscal year.

3.4 Frequency for Review of the Standards Prioritization Process

The SWG Chair shall ensure that the SWG reviews the Standards Prioritization Process at least annually to determine if any changes are necessary and revises the process as needed.

This page intentionally left blank.

4 DEFINITIONS

CSO Standards DAA — The authority to approve CSO standards has been delegated jointly to the Chief Information Security Officer (CISO) and Director of the Office of Information Systems (OIS). For the purposes of this process, they are referred to as the CSO Standards DAA.

Existing Cyber Security Standard — A category that includes standards that are currently effective and published on the CSO Standards web page. This does not include updates to standards, which address changes associated with newer technology (e.g., releases of new software versions), as these revisions are considered to be New Cyber Security Standards. Refer to the definition for New Cyber Security Standards for additional information.

External Standard — A cyber security standard (e.g., a configuration baseline or set of requirements for the use of a technology or technologies) developed by a U.S. Government (USG) agency (e.g., CNSS, Defense Information Systems Agency (DISA), National Security Agency (NSA), NIST), private organization (e.g., Center for Internet Security (CIS)), or a software / hardware vendor. External standards are used by the NRC as the basis for NRC cyber security standards.

Information System — A compilation of hardware, software, and firmware that processes electronic information to achieve a particular purpose.

ISSO Forum — A forum established by NRC for the purpose of providing a communication mechanism for CSO staff and Information System Security Officers (ISSOs) to communicate, collaborate, and exchange information relevant to the NRC cyber security program.

New Cyber Security Standard — A category that includes new cyber security standards to be created (i.e., standards not currently in existence), as well as certain revisions to existing standards. This refers specifically to revisions necessary to address newer technologies or software product versions.

Standards Working Group (SWG) — A working group established by NRC for the purpose of evaluating, recommending, and communicating information technology standards, checklists, and guidance for use at NRC.

SWG Chair — The position of SWG chair is filled by the CSO Policies, Standards, and Training Senior Information Technology Security Officer (SITSO) or his/her designee. The SWG chair provides vision, leadership, direction, and oversight of the SWG at the direction of the CISO.

SWG FY Standards Priorities — The prioritized list of new standards to be developed and existing standards to be revised for the fiscal year produced as a result of the final step of the Standards Prioritization Process. The prioritized list must be concurred on by the SWG and approved by the CSO Standards DAA.

This page intentionally left blank.

5 ACRONYMS

CIS	Center for Information Security
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CSO	Computer Security Office
CUI	Confidential Unclassified Information
DAA	Designated Approving Authority
DEDO	Deputy Executive Director for Operations
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISSO	Information System Security Officer
IT	Information Technology
IM	Information Management
NRC	Nuclear Regulatory Commission
NIST	National Institute for Standards and Technology
NSA	National Security Agency
OIS	Office of Information Services
OMB	Office of Management and Budget
SITSO	Senior Information Technology Security Officer
SGI	Safeguard Information
SP	Special Publication
STIG	Security Technical Implementation Guide
SWG	Standards Working Group

TRM	Technical Reference Manual
USG	U.S. Government
VoIP	Voice over Internet Protocol

6 REFERENCES

- NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, as revised

CSO-PROS-3001 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
27-Nov-12	1.0	Initial issuance	ISSO Forum announcement and posting to CSO web page	As needed

APPENDICES

APPENDIX A – New Standards Prioritization Criteria

New Standards Prioritization Criteria	Point Value
Associated with a DAA (DEDO, CISO, Director of OIS) priority	15
Associated with an IT/IM Roadmap/Strategy initiative	5
Driven by a federally mandated requirement	5
Affects the following number of ***computing assets*** (currently or projected within the next 24 months):	
• 5000 or greater	12
• 2500 – 4999	10
• 1000 – 2499	8
• 500 – 999	5
• 250 – 499	3
• 50 – 249	2
• 1 – 49	1
Affects the following number of ***users*** (currently or projected within the next 24 months):	
• 2500 or greater	10
• 1000 – 2499	8
• 500 – 999	5
• 250 – 499	3
• 50 – 249	2
• 1 – 49	1
Standards status for evalution candidate:	
• No internal CSO standards exist, but external standards do exist	5
• Neither internal CSO standards ***nor*** external standards exist	10
Affects information systems which process safeguards information (SGI) or classified data	5
The high water mark (i.e., maximum impact value) security categorization for information resident on a system is High	5
There are security components that provide perimeter or endpoint protection	5
Upcoming deployment for the technologies or products covered (new or upgrade) within the next 24 months	5
There are cyber security issues with the configuration currently in use	5
Maximum Possible Points	**82**

This page intentionally left blank.

APPENDIX B – Existing Standards Prioritization Criteria

Existing Standards Prioritization Criteria	Point Value
Associated with a DAA (DEDO, CISO, Director of OIS) priority	15
Associated with an IT/IM Roadmap/Strategy initiative	5
Driven by a federally mandated requirement	5
Affects the following number of ***computing assets*** (currently or projected within the next 24 months):	
• 5000 or greater	12
• 2500 – 4999	10
• 1000 – 2499	8
• 500 – 999	5
• 250 – 499	3
• 50 – 249	2
• 1 – 49	1
Affects the following number of ***users*** (currently or projected within the next 24 months):	
• 2500 or greater	10
• 1000 – 2499	8
• 500 – 999	5
• 250 – 499	3
• 50 – 249	2
• 1 – 49	1
Affects information systems which process SGI or classified data	5
The high water mark (i.e., maximum impact value) security categorization for information resident on a system is High	5
There are security components that provide perimeter or core endpoint protection	5
Upcoming deployment for the technologies or products covered (new or upgrade) within the next 24 months	5
Significant number of updates (e.g., more than 3) or rewrite of the external standard(s) from the version used to develop or revise the effective CSO standard	5
There are cyber security issues with the configuration currently in use	5
Maximum Possible Points	**77**

This page intentionally left blank.

APPENDIX C – Description of Evaluation Candidate Attributes

The following table lists and describes evaluation candidate attributes. These attributes are needed for each evaluation candidate in order for the SWG to score the candidate against its applicable criteria specified in Section 3.2.

Name	Type	Description
Associated DAA Priority	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one DAA priority. DAA priorities can include those issued by the Deputy Executive Director for Operations (DEDO), Chief Information Security Officer (CISO), or Director of the Office of Information Services (OIS). Example: If the NRC DAA stated that virtualization was a DAA priority, then an evaluation candidate covering enterprise virtualization software to be used to fulfill that goal (e.g., VMware) would be considered to be associated with a DAA priority.
Associated IT/IM Roadmap or Strategy Initiative	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one IT/IM Roadmap or IT/IM Strategy initiative (e.g., goal or theme). Example: The FY08-FY13 IT Roadmap includes goals for increasing support for mobile computing devices and responding to the needs of the NRC's mobile workforce. Based on this, an evaluation candidate covering agency laptops would be considered to be associated with an IT/IM Roadmap/Strategy Initiative.
Associated Federally Mandated Requirement	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one federally mandated requirement. Federally mandated requirements can include, but are not restricted to, OMB mandates, Executive Orders, and Federal Information Processing Standard (FIPS) requirements. Example: OMB M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)* (and later issuances from OMB) mandate transition dates for agencies to move to IPv6. Based on this, an evaluation candidate covering IPv6 (e.g., security for transition methods) would be considered to be associated with a federally mandated requirement.
Number of NRC Computing Assets Affected	Number	The number of NRC computing assets (e.g., workstations, mobile devices, network devices, servers, appliances), which may be either physical or virtual (e.g., a virtual machine) that would be affected by the evaluation candidate. This includes owned and leased equipment for NRC information systems. Estimates are acceptable if it is not possible to determine the actual number. Example: An evaluation candidate for a revision to the NRC Organization Defined Values associated with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* would likely affect all NRC computing assets, physical or virtual. Thus, the attribute value would be the count (actual or estimate) of the number of NRC computing assets.

Name	Type	Description
Number of NRC Users Affected	Number	The number of NRC users (contractors or employees) that would be affected by the evaluation candidate. The term user applies not just to end users of a cyber product, for example, but also to NRC administrators and support personnel. Estimates are acceptable if it is not possible to determine the actual number. Example: Assuming that NRC uses the Microsoft Windows Server 2008 Revision 2 operating system for all centralized Windows authentication (e.g., on workstations at NRC, through Citrix), an evaluation candidate covering that operating system version would affect all NRC users who use NRC Windows workstations and/or use Citrix for remote access.
Associated with Information System(s) that Process or Store SGI or Classified Data	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one information system that processes or stores SGI or classified data. Example: Evaluation candidates covering laptops specifically for SGI or classified environments; NRC Organization Defined Values for NIST SP 800-53; or electronic media/device handling would be considered to be associated with at least one information system that processes or stores SGI or classified data.
Published CSO Standard	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one CSO standard (e.g., CSO-STD-XXXX) that is published and is currently in effect (per the CSO standards web page). Example: Assuming that there was not a published and effective CSO standard covering Microsoft Windows Server 2012, then an evaluation candidate covering the operating system version would not be considered to be associated with a published CSO standard.
Published External Standard	Boolean: True or False	Specifies whether the evaluation candidate is associated with at least one external standard (e.g., Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) or Center for Internet Security (CIS) Benchmark) that is published and finalized. Draft external standards do not qualify. For evaluation candidates that cover cyber products, the external standard must be written for the major version of the cyber product to qualify. Example: Assuming that an external standard does not exist for major version 10.8 of the Mac OS X operating system, then an evaluation candidate covering the operating system version would not be considered to be associated with a published external standard. An external standard was published and finalized for major version 10.7 of Mac OS X would not be sufficient since it is written for different major version of the operating system.

Name	Type	Description
Highest Security Categorization for Associated Information System(s)	High, Moderate, or Low	Specifies the highest overall security categorization for all information systems associated with the evaluation candidate. Example: Assuming that major version 5 of the Red Hat Enterprise Linux operating system is used in two NRC information systems, with one having an overall security categorization of moderate and the second having a categorization of high, then the highest overall security categorization for an evaluation candidate covering the operating system version would be high.
Network Perimeter Protection	Boolean: True or False	Specifies whether the evaluation candidate, such as a cyber product or category, covers network perimeter protection. This can include protection varying from stateful packet inspection (e.g., a basic firewall) to tailored application gateways (e.g., a mail gateway) or application firewalls (e.g., a web application firewall). Example: Evaluation candidates, such as intrusion prevent systems, firewalls, mail gateways, or web application firewalls, positioned at the perimeter of the NRC production network (e.g., for public web applications) or on the perimeter of an externally hosted information system would be considered to be providing network perimeter protection.
Endpoint Protection	Boolean: True or False	Specifies whether the evaluation candidate, such as a cyber product or category, covers endpoint protection. This can include, but is not restricted to, the following host endpoint protection examples: host firewall, host intrusion detection/prevention system, anti-malware, file integrity checking, or application white listing. Example: Evaluation candidates, such as the anti-malware cyber category or a specific anti-malware cyber product for endpoints, would be considered to be providing endpoint protection.
Upcoming Deployment	Boolean: True or False	Specifies whether the evaluation candidate, such as a cyber product or category, is associated with an upcoming major deployment within the next 24 months. Deployments may be to transition away from existing cyber products or to roll out new cyber products to fulfill a new purpose. Example: Assuming that the NRC is moving away from the Microsoft Windows XP operating system with an upcoming major deployment of Microsoft Windows 7 in less than 24 months, then an evaluation candidate covering Windows 7 would be considered to be associated with an upcoming deployment.

Name	Type	Description
Number of Releases to External Standard(s)	Number	Specifies the number of releases to the associated external standard(s) for the cyber product or category from the version(s) used to develop or revise the effective CSO standard. Draft releases of external standards shall not be considered. Example: Assuming that the effective CSO standard for Microsoft Windows 7 was developed using version 1 release 1 of the external standard, which is a DISA STIG, and the latest release is version 1 release 9, then there have been 8 releases to the external standard associated with evaluation candidate Windows 7.
Rewrite of External Standard(s)	Boolean: True or False	Specifies whether there has been a rewrite to the associated external standard(s) for the cyber product or category from the version(s) used to develop or revise the effective CSO standard. Draft releases of external standards shall not be considered. Rewrites includes new external standards that takes the place of the existing external standard (e.g., when DISA has transition from a security checklist for a STIG for a specific product) and significant updates that wholly change the external standard. A common example of the latter is when a CIS Benchmark is rewritten and a new major version (e.g., going from version 1.1 to 2.0) of the standard is released without an accompanying revision history. Example: Assuming that the effective CSO standard for Microsoft SQL Server 2005 was developed using version 1.1.0 of the external standard, which is a CIS Benchmark, and the latest release is version 2.0.0, which is a major release and does not include a revision history of changes, then evaluation candidate SQL Server 2005 would be considered to have a rewrite of the associated external standard.
Cyber Security Issue(s) with the Configuration Currently in Use	Boolean: True or False	Specifies whether there is a cyber security issue(s) with the current configuration, which may be specified in an existing CSO standard. This may include a configuration that does not include specific requirements needed to prevent known attacks or a configuration that includes a requirement that is known to present unacceptable to risk. Example: Assuming that there is a configuration for a mail gateway that did not require the blocking of known spoofed emails from external parties or if there was a configuration for a directory server that permitted clear text transmission of authentication credentials over the network, then evaluation candidates associated with the associated mail gateways or directory servers (either through cyber categories or for the specific cyber products) would be considered to have a cyber security issue with the configuration currently in use.

APPENDIX D – Seven Step Prioritization Process Walkthrough

This appendix includes a simplified, practical walkthrough of the seven steps process in Section 3.1.

Step 1: Identify Evaluation Candidates

a. The SWG Chair enlists the help of SWG members, as well as other NRC program and support offices as needed, and identifies the following evaluation candidates in the two evaluation groups (for illustrative purposes, only a small set of candidates is listed):

   New Cyber Security Standards Evaluation Group

   i. Network Devices/Infrastructure
   ii. Voice over Internet Protocol (VoIP)
   iii. Confidential Unclassified Information (CUI)
   iv. Oracle PeopleSoft
   v. Microsoft Windows Server 2008 Release 2 (R2)
   vi. Remote Access
   vii. SGI Laptop
   viii. Red Hat Enterprise Linux 5
   ix. Red Hat Enterprise Linux 6

   Existing Cyber Security Standards Evaluation Group

   i. Organization Defined Values
   ii. Electronic Media and Device Handling
   iii. System Back-up

b. After obtaining input from the SWG, the SWG Chair exercises his/her discretion and groups Red Hat Enterprise Linux versions 5 and 6 together as a grouped evaluation candidate within the New Cyber Security Standards evaluation group. The SWG Chair does not elect to group any evaluation candidates together within the Existing Cyber Security Standards evaluation group.

Step 2: Research, Score, and Rank Candidates

a. SWG members assist the SWG Chair in identifying the evaluation candidates' attribute values using APPENDIX C – Description of Evaluation Candidate Attributes.

b. The SWG Chair ensures that the SWG scores each evaluation candidate in accordance with the criteria in Section 3.2. The results of the scoring are (in order, by evaluation group):

   New Cyber Security Standards Evaluation Group

   i. Network Devices/Infrastructure: 60 points

ii. Remote Access: 55 points
iii. VoIP: 47 points
iv. Microsoft Windows Server 2008 R2: 33 points
v. CUI: 32 points
vi. Oracle PeopleSoft: 16 points
vii. Red Hat Enterprise Linux 5 and 6: 16 points
viii. SGI Laptop: 12 points

Existing Cyber Security Standards Evaluation Group

i. Organization Defined Values: 47 points
ii. Electronic Media and Device Handling: 37 points
iii. System Back-up: 32 points

Since the scores are presented in order (with the highest score having the top rank), this also provides the relative rank for each candidate among all of the candidates within each evaluation group.

Step 3: Review Initial Scoring Results

a. The SWG reviews the results from Step 2.

i. New Cyber Security Standards evaluation group: The ranking list for this group includes a tie where the Red Hat Enterprise Linux 5 and 6, and Oracle PeopleSoft evaluation candidates have the same score of 16 points.

ii. Existing Cyber Security Standards evaluation group: No ties exist for evaluation candidates in this group.

b. Based on the ranking identified, the SWG, at the discretion of the SWG Chair, has a second opportunity to group multiple closely related evaluation candidates together as one grouped evaluation candidate. The SWG does not opt to further group any of the candidates due to the lack of a strong relationship or interdependency between candidates in either evaluation group.

Step 4: Re-Score Candidates (if applicable)

a. Since the SWG did not opt to group any evaluation candidates in either evaluation group, the SWG does not re-score any candidates.

Step 5: Break Ties and Re-Rank (if applicable)

Note: This step is applicable because the SWG discovered a tie in Step 3.

New Cyber Security Standards Evaluation Group:

a. The SWG Chair breaks the tie between the Red Hat Enterprise Linux 5 and 6, and Oracle PeopleSoft evaluation candidates by ranking Oracle PeopleSoft ahead of Red Hat Enterprise Linux 5 and 6 due to the financial significance of Oracle PeopleSoft. Oracle PeopleSoft provides payroll and general ledger capabilities.

b. The SWG re-ranks the list of candidates to include the results of the tie breaking. The new ranking is listed below. This does not affect the ranking for the candidates in the Existing Cyber Security Standards evaluation group.

   i. Network Devices/Infrastructure
   ii. Remote Access
   iii. VoIP
   iv. Microsoft Windows Server 2008 R2
   v. CUI
   vi. Oracle PeopleSoft
   vii. Red Hat Enterprise Linux 5 and 6
   viii. SGI Laptop

Existing Cyber Security Standards Evaluation Group:

a. No ties exist for candidates in this evaluation group. Since no ties exist, the SWG does not need to break any ties or re-rank candidates.

Since all ties have been broken and each candidate has a unique rank within each evaluation group, the SWG proceeds to Step 6.

Step 6: Consider Current SWG Projects

New Cyber Security Standards Evaluation Group:

a. The SWG identifies one current SWG project to develop a new standard, which is not on schedule to be finished prior to the beginning of the upcoming fiscal year when the prioritization results will be implemented. The SWG project is to develop a CSO standard for the Sybase Adaptive Server Enterprise database server cyber product.

b. The SWG discusses the financial impact and percentage complete of the current SWG project, and technology lifecycle of the cyber product to determine whether to continue, postpone, or stop the project.

   The SWG discovers that the NRC is reducing the use of Sybase in favor of other database server products.

c. Based on SWG input, the SWG Chair decides to postpone the project to develop a CSO standard for the Sybase Adaptive Server Enterprise database server product. The SWG Chair recommends that the SWG revisit the project during the next iteration of the prioritization process, especially if it turns out that the reduction in use of Sybase does not occur as planned.

   Since the SWG Chair, with the input of SWG members, decided to postpone the project there is no impact to the ranking of candidates associated with this evaluation group in Steps 5.

Existing Cyber Security Standards Evaluation Group:

a. No issues exist since all projects to revise existing cyber security standards for the current fiscal year are on or ahead of schedule.

Step 7: Establish SWG Priorities

a. The SWG is obligated to review, at a minimum, the top 25% of highest ranked candidates in the New Cyber Security Standards evaluation group and the top 15% of highest ranked candidates in the Existing Cyber Security Standards evaluation group in order to establish SWG priorities for the fiscal year.

   i. The top 25% of the highest ranked candidates in the New Cyber Security Standards evaluation group include the top ranked Network Devices/Infrastructure candidate and the Remote Access candidate.

   ii. The top 15 % of the highest ranked candidates in the Existing Cyber Security Standards evaluation group includes the top ranked Organization Defined Values candidate.

b. The SWG Chair collaborates with SWG members and analyzes historical data to estimate the time required (in hours) to develop standards for the top ranked evaluation candidates. The SWG Chair develops the following time estimates for candidates in each evaluation group.

   New Cyber Security Standards Evaluation Group:

   i. The SWG will require 600 cumulative hours to develop a CSO standard for the Network Devices/Infrastructure candidate.

   ii. The SWG will require 450 cumulative hours to develop a CSO standard for the Remote Access candidate.

   Existing Cyber Security Standards Evaluation Group:

   i. The SWG will require 350 cumulative hours to develop a revised CSO standard for the Organization Defined Values candidate.

   Note: The estimates above are not intended to be a representation of the actual amount of time necessary to develop a new cyber security standard.

The two candidates in the New Cyber Security Standards evaluation group will require a total of 1050 hours. This results in a total of 1400 hours when added to estimate of 350 hours for the candidate in the Existing Cyber Security Standards evaluation group.

i. The time (1050 hours) required for the candidates in the New Cyber Security Standards evaluation group is exactly 75% of the total time (1400 hours) required for the SWG.

ii. The time (350 hours) required for the candidates in the Existing Cyber Security Standards evaluation group is exactly 25% of the total time (1400 hours) required for the SWG.

The estimates of total time for each evaluation group fall within the goals for allocating time to each group, which are specified in section 2.2 Evaluation Groups.

c. The SWG Chair documents the prioritized lists of new standards to be developed and existing standards to be revised for the fiscal year.

Prioritized List of New Cyber Security Standards:

i. Development of a Network Devices/Infrastructure CSO standard

ii. Development of a Remote Access CSO standard

Prioritized List of Existing Cyber Security Standards:

i. Revision of the Organization Defined Values CSO standard

Note: The prioritized lists above are the two components of the SWG FY Standards Priorities document referenced in Step 7 of the process.

d. The SWG Chair facilitates a vote by the SWG in accordance with the SWG Charter for the SWG FY Standards Priorities.

e. Following the SWG's vote to approve, the SWG SITSO provides the SWG FY Standards Priorities to the CSO Standards DAA for review and approval.

f. After the CSO Standards DAA approves the SWG FY Standards Priorities, the SWG Chair uses the approved priorities to lead, direct, and oversee operations of the SWG for the fiscal year.