

## **Consideration of Comments for Project 2008-14 — Cyber Security Violation Severity Levels (CIP Version 1 VSLs and SAR revision)**

The Cyber Security Violation Severity Levels Drafting Team thanks all commenters who submitted comments on the CIP Version 1 VSLs and SAR revision. The Version 1 VSLs and the revised SAR were posted for a 30-day public comment period from March 16, 2009 through April 20, 2009. Stakeholders were asked to provide feedback through a Word document Comment Form. There were 12 sets of comments, including comments from more than 60 different people from over 45 companies representing 7 of the 10 Industry Segments as shown in the table on the following pages.

While the comment form addressed VSLs for the Version 1 Cyber Security Standards and the SAR for that project as well as the VSLs and VRFs for the Version 2 Cyber Security Standards, this report addresses only the VSLs and SAR for the Version 1 Cyber Security Standards. Comments related to the VSLs and VRFs for the Version 2 Cyber Security Standards will be addressed in a separate report.

For this report, stakeholder comments were sorted so that it is easier to see all comments related to each set of VSLs. All comments have been posted in their original format at the following site:

[http://www.nerc.com/filez/standards/Project2008-14\\_Cyber\\_Security\\_VSLDT.html](http://www.nerc.com/filez/standards/Project2008-14_Cyber_Security_VSLDT.html)

Based on stakeholder comments, the drafting team did not make any changes to the SAR, but did make some changes to several of the sets of VSLs for CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, and CIP-007-1. No changes were made to VSLs for CIP-008-1 or for CIP-009-1. Most changes were either clarifying or format changes. In some cases, stakeholders identified additional descriptions of noncompliant performance that could be used to add more options to the already proposed VSLs – and where the proposed VSLs met the definitions for the proposed VSL category, the proposed VSLs were adopted.

Some stakeholders are opposed to setting noncompliance with a binary requirement or subrequirement as a “Severe” VSL. If an entity is totally noncompliant with a requirement, then this meets the criteria for a “Severe” VSL.

Some stakeholders commented that the drafting team should have developed a single set of VSLs for a requirement and its associated subrequirements. The drafting team agrees that having a single set of VSLs for each requirement, in its entirety, is preferable, however, in accordance with the directives in FERC's VSL Order, the drafting team has assigned a set of VSLs to each requirement and each subrequirement that has a VRF. While we understand that NERC is trying to obtain endorsement to assign a single set of VSLs to each requirement in its entirety, the VSLs for the Version 1 Cyber Security standards need to be filed before FERC will have had a chance to review NERC's proposal for assigning a single VRF and a single set of VSLs for each requirement in its entirety. Note that there are a few exceptions where the drafting team felt it could reasonably use a “roll-up” approach to VSLs, it did so. Where both the requirement and the subrequirement have sets of VSLs, the team has taken care to develop VSLs that should not result in double jeopardy.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards,

Gerry Adamski, at 609-452-8060 or at [gerry.adamski@nerc.net](mailto:gerry.adamski@nerc.net). In addition, there is a NERC Reliability Standards Appeals Process.<sup>1</sup>

---

<sup>1</sup> The appeals process is in the Reliability Standards Development Procedures:  
<http://www.nerc.com/standards/newstandardsprocess.html>.

**Index to Questions, Comments, and Responses**

- 1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision. .... 9
- 4. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here. ....38
- 5. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?.....79

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

The Industry Segments are:

- 1 — Transmission Owners
- 2 — RTOs, ISOs
- 3 — Load-serving Entities
- 4 — Transmission-dependent Utilities
- 5 — Electric Generators
- 6 — Electricity Brokers, Aggregators, and Marketers
- 7 — Large Electricity End Users
- 8 — Small Electricity End Users
- 9 — Federal, State, Provincial Regulatory or other Government Entities
- 10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
1.	Group 1	Ben Li	IRC Standards Review Committee		X									
2.	Group 1	Charles Yeung	SPP		X									
3.	Group 1	Patrick Brown	PJM		X									
4.	Group 1	Lourdes Estrada-Saliner	CAISO		X									
5.	Group 1	James Castle	NYISO		X									
6.	Group 1	Steve Myers	ERCOT		X									
7.	Group 1	Matt Goldberg	ISO-NE		X									
8.	Group 1	Bill Phillips	MISO		X									
9.	Individual	Chris Scanlon	Exelon	X										
10.	Individual	Dan Rochester	IESO		X									

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
11.	Group 2	Denise Koehn	Bonneville Power Administration	X										
12.	Group 2	Huy Ngo	Control Cntr HW Design & Maint	X										
13.	Group 2	Allen Chan	General Counsel	X		X		X	X					
14.	Group 2	Robin Chung	Generation Support			X		X	X					
15.	Group 2	Sheree Chambers	Power Scheduling Coordination			X		X	X					
16.	Group 2	Tina Weber	Power Scheduling Coordination			X		X	X					
17.	Group 2	Pete Jeter	Security & Emergency Response	X		X		X	X					
18.	Group 2	Erik Smith	Security & Emergency Response	X		X		X	X					
19.	Group 2	Dick Winters	Substation Operations	X										
20.	Group 2	Curt Wilkins	Transmission System Operations	X										
21.	Group 2	Kelly Hazelton	Transmission System Operations	X										
22.	Group 2	Jim Domschot	Transmission Work Planning and Evaluation	X										
23.	Group 2	Jim Jackson	Transmission Work Planning and Evaluation	X										
24.	Group 2	Kevin Dorning	Tx PSC Technical Services	X										
25.	Individual	Greg Rowland	Duke Energy	X		X		X	X					
26.	Group 3	Guy Zito	Northeast Power Coordinating Council											X
27.	Group 3	Ralph Rufrano	New York Power Authority					X						
28.	Group 3	Rick White	Northeast Utilities	X										

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

		Commenter	Organization	Industry Segment											
				1	2	3	4	5	6	7	8	9	10		
29.	Group 3	Chris de Graffenried	Consolidated Edison Com. Of New York, Inc.	X											
30.	Group 3	David Kiguel	Hydro One Networks Inc.	X											
31.	Group 3	Randy MacDonald	New Brunswick System Operator		X										
32.	Group 3	Roger Champagne	Hydro-Quebec TransEnergie		X										
33.	Group 3	Tony Elacqua	New York Independent System Operator		X										
34.	Group 3	Manny Couto	National Grid	X											
35.	Group 3	Kathleen Goodman	ISO - New England		X										
36.	Group 3	Brian Evans-Mongeon	Utility Services, LLC						X						
37.	Group 3	Mike Garton	Dominion Resources Services					X							
38.	Group 3	Chris Orzel	FPL/NextEra					X							
39.	Group 3	Sylvain Clermont	Hydro-Quebec TransEnergie	X											
40.	Group 3	Kurtis Chong	Independent Electricity System Operator		X										
41.	Group 3	Lee Pedowicz	Northeast Power Coordinating Council												X
42.	Group 3	Gerry Dunbar	Northeast Power Coordinating Council												X
43.	Group 3	Mike Gildea	Constellation Energy						X						
44.	Group 3	Michael Schiavone	National Grid	X											
45.	Group 3	Brian Hogue	Northeast Power Coordinating Council												X

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

		Commenter	Organization	Industry Segment																
				1	2	3	4	5	6	7	8	9	10							
46.	Group 4	Michael Brytowski	MRO NERC Standards Review Subcommittee																	X
47.	Group 4	Carol Gerou	MP	X		X		X	X											
48.	Group 4	Neal Balu	WPS			X	X	X	X											
49.	Group 4	Terry Bilke	MISO		X															
50.	Group 4	Joe DePoorter	MGE			X	X	X	X											
51.	Group 4	Ken Goldsmith	ALTW				X													
52.	Group 4	Jim Haigh	WAPA	X						X										
53.	Group 4	Terry Harbour	MEC	X		X		X	X											
54.	Group 4	Joseph Knight	GRE	X		X		X	X											
55.	Group 4	Scott Nickels	RPU			X	X	X	X											
56.	Group 4	Dave Rudolph	BEPC	X		X		X	X											
57.	Group 4	Eric Ruskamp	LES	X		X		X	X											
58.	Group 4	Pam Sordet	XCEL	X		X		X	X											
59.	Individual	Michael J. Sonnelitter	NextEra Energy Resources, LLC					X												
60.	Individual	Michael Gammon	Kansas City Power & Light	X		X		X	X											
61.	Individual	Paul McClay	Tampa Electric Company	X		X		X	X											
62.	Individual	Thad Ness	American Electric Power (AEP)	X		X		X	X											

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

---

		Commenter	Organization	Industry Segment										
				1	2	3	4	5	6	7	8	9	10	
63.	Individual	Michael P Mertz	Southern California Edison Company	X		X		X	X					

- \*Group 1 — IRC Standards Review Committee
- \*Group 2 — Bonneville Power Administration
- \*Group 3 — Northeast Power Coordinating Council
- \*Group 4 — MRO NERC Standards Review Subcommittee

1. Please review all of the proposed VLS for CIP-002-1 through CIP-009-1 (version 1 standards). Then in the following table, please provide alternate language for any VSLs that you disagree with. Please be sure to identify the standard number and requirement number for each proposed revision.

**CIP-002-1 – Critical Cyber Asset Identification**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-002-1. The drafting team adopted the proposed modifications for R1.1 and a suggestion to modify R4 to improve clarity. In addition, based on comments suggesting that the VSLs for R3 didn't match the language in the requirement, the drafting team modified the VSLs for R3 to more closely use the same language as is used in the requirement. A typographical error in the High VSL for R4 was also corrected. All changes made to the VSLs are shown in the first table – and the modifications that were proposed are shown in the second table below.

Summary of Changes Made to VSLs for CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R1.1	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology does not include procedures but includes evaluation criteria.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but not evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
Revised R1.1	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology <b>that includes evaluation criteria, but does not include procedures.</b>	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but <b>does not include</b> evaluation criteria.	The Responsible Entity did not maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
Original R3	N/A	N/A	The Responsible Entity has developed a list of Critical Cyber Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Cyber Assets even if such list is null.
Revised R3.	N/A	N/A	The Responsible Entity has developed a list of <b>associated</b> Critical Cyber Assets <b>essential to</b>	The Responsible Entity did not develop a list of <b>associated</b> Critical Cyber Assets <b>essential to the</b>

Summary of Changes Made to VSLs for CIP-002-1 Critical Cyber Asset Identification				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
			the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	operation of the Critical Asset list as per requirement R2 even if such list is null.
Original R4.	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
Revised R4.	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets (even if the list is null). <b>OR</b> The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if the list is null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

All Changes Proposed by Stakeholders for VSLs for CIP-002-1 Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<p><i>Comment: R1 is poorly structured. Comment on VSL can only be made based on how it's written, not how it should be written. VSL for R1 is binary, which it shouldn't be. It is a good example of how inappropriate to have a binary requirement while its subrequirements' VSLs are a mixture of binary and graded.</i></p>			
<p><b>Response:</b> Modifying the requirement is outside the scope of this project. There is another drafting team that is working on revising the requirements in the set of Cyber Security standards.                      The drafting team made total noncompliance with the requirement a Severe VSL to prevent double jeopardy. Because R1 could easily be subdivided into more than one requirement, the team elected to give the primary requirement and its main subrequirements their own sets of VSLs.</p>					
SoCal	R1			The responsible entity has documented a risk-based assessment methodology but has not applied it to identify its Critical Assets as specified in R1.	<del>The responsible entity has documented a risk-based assessment methodology but has not applied it to identify its Critical Assets as specified in R1.</del>
<p><b>Response:</b> The suggestion to shift the sole VSL from Severe to High was not adopted. Where a requirement is "binary" in nature, the VSL is not conducive to a graded severity level, therefore a failure to perform the task identified in the requirement can only be classified as "severe".</p>					
Tampa Electric	R1				<p>Comment: If the RE did not include all asset types listed in R1.2.1 through R1.2.7 it is a severe VSL. Some entities will not have all of these asset types to consider.</p> <p><b>Suggested wording:</b> The Responsible Entity did not consider all applicable asset types listed in R1.2.1 through R1.2.7 in its risk-based assessment.</p>
<p><b>Response:</b> The suggestion was not adopted. The DT does not agree that the VSL implies all asset types must be considered.</p>					

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-002-1 Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Duke Energy	R1.1		The Responsible Entity maintained documentation describing its risk-based assessment methodology which includes evaluation criteria, but does not include procedures.		
<b>Response:</b> The alternative suggested was adopted by the drafting team.					
IRC SRC, IESO	R1.1	<i>Comment: Graded, but not based on the failure of its subrequirements.</i>			
<b>Response:</b> There are no sub-sub requirements for R1.1 so the drafting team cannot interpret this comment.					
SoCal	R1.1	N/A	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes evaluation criteria but does not include procedures.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that includes procedures but does not include evaluation criteria.	The Responsible Entity maintained documentation describing its risk-based assessment methodology that did not include procedures and evaluation criteria.
<b>Response:</b> The alternatives suggested for R1.1 Moderate and High VSLs were adopted, but not the proposed alternative for the Severe VSL as the VSL proposed by the drafting team covers the scenario where there is no methodology as well as the scenario where there is a methodology and it is missing both the procedures and the evaluation criteria.					
IRC SRC, IESO	R1.2, R1.21-1.27	<i>Comment: VSL for R1.2 is binary, which could be graded depending on the failure to meet any of its subrequirements.</i>			
<b>Response:</b> Many responsible entities may own only one of the asset types listed, therefore the suggestion to make this a graded VSL was not adopted.					
IRC SRC, IESO	R2	<i>Comment: OK, but the last part “even if such list is null” seems irrelevant.</i>			

All Changes Proposed by Stakeholders for VSLs for CIP-002-1 Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> The subject phrase was included for clarity.</p>					
IRC SRC, IESO	R3	<p><i>Comment: The VSLs for R3 should be graded to also cover the Low and Moderate columns since it has subrequirements R3.1 to R3.3 all of which need to be met fully comply with R3. Further, the last part “even if such list is null” under the Severe condition seems irrelevant.</i></p>			
<p><b>Response:</b> The drafting team could not identify noncompliant performance that would meet the criteria for Lower and Moderate without also duplicating the VSLs developed for the subrequirements. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy. The subject phrase, “even if such list is null” was included for clarity.</p>					
Tampa Electric	R3	<p><i>Comment: Lack of inclusion of a single critical cyber asset on the list, regardless of whether that asset is effectively protected under the requirements of the standards is a severe VSL under several of the sub-requirements, which is the same as not having a list at all. We recommend moving this to Lower level. Consideration should be given as to whether that was due to a documentation error, or if the asset has been protected. Also, realize that if it is documented as a cyber asset rather than a critical cyber asset it still must be protected under the standards.</i></p>			
		<p>Less than 5% of Cyber Assets essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.</p>	5% to 10%	10% - 20%	Greater than 20%
<p><b>Response:</b> The alternative suggested for R3 was not adopted. The set of VSLs proposed by the drafting team avoided addressing noncompliance with the subrequirements, as these have their own VSLs and to include the subrequirements in both the primary requirement and the subrequirements would lead to double jeopardy.</p>					
IRC SRC, IESO	R3.1 R3.2 R3.3	<p><i>Comment: Binary; OK.</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-002-1 Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R3.1			A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.	Two or more Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
SoCal	R3.2			A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.	Two or more Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
SoCal	R3.3			A Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.	Two or more Cyber Asset essential to the operation of the Critical Asset was identified that met the criteria in this requirement but was not included in the Critical Cyber Asset List.
<p><b>Response:</b> The alternatives suggested for R3.1, R3.2, and R3.3 were not adopted. If the responsible entity does identify a Cyber Asset but the asset is not on the list, then from a compliance perspective, the asset has not been identified. The measure for this requirement is specific that the responsible entity must have a "list." These subrequirements are binary and failure to meet these subrequirements is Severe.</p>					
IRC SRC, IESO	R4	<i>Comment: OK.</i>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
SoCal	R4	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of the list of Critical Assets (even if such list is null)	

All Changes Proposed by Stakeholders for VSLs for CIP-002-1 Critical Cyber Asset Identification					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
				OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of the list of the list of Critical Cyber Assets	
<p><b>Response:</b> The drafting team adopted the proposed reformatting for the High VSL.</p>					

**CIP-003-1 Security Management Controls**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-003-1. The drafting team adopted several of the proposed modifications. All changes made to the VSLs were made based on stakeholder comments and are shown in the first table – and the modifications that were proposed by stakeholders are shown in the second table below.

Summary of Changes Made to VSLs for CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R2.1	N/A	N/A	N/A	The senior manager is not identified by name, title, business phone, business address, and date of designation.
Revised R2.1	N/A	The senior manager is identified by name, title, and date of designation but the designation is missing business phone or business address	The senior manager is identified by business phone and business address but the designation is missing one of the following: name, title, or date of designation	The senior manager is not identified by name, title, business phone, business address, and date of designation.
Original R2.2	N/A	N/A	N/A	Changes to the senior manager were not documented within thirty calendar days of the effective date.
Revised R2.2	Changes to the senior manager were documented in greater than 30 but less than 60 days of the effective date.	Changes to the senior manager were documented in 60 or more but less than 90 days of the effective date.	Changes to the senior manager were documented in 90 or more but less than 120 days of the effective date.	Changes to the senior manager were documented in 120 or more days of the effective date.
Original R3.2	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include <b>either</b> :	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include <b>both</b> :

Summary of Changes Made to VSLs for CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
			1) an explanation as to why the exception is necessary, or 2) any compensating measures or a statement accepting risk.	1) an explanation as to why the exception is necessary, and 2) any compensating measures or a statement accepting risk.
Revised R3.2	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary. OR The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but the exception did not include any compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary, nor did it include any compensating measures or a statement accepting risk.
Original R4	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement but documented a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.
Revised R4	N/A	The Responsible Entity implemented but did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	The Responsible Entity did not implement nor document a program to identify, classify, and protect information associated with Critical Cyber Assets.

Summary of Changes Made to VSLs for CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R5	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement but documented a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
Revised R5	N/A	The Responsible Entity implemented but did not document a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	The Responsible Entity did not implement nor document a program for managing access to protected Critical Cyber Asset information.
Original R5.1	N/A	N/A	N/A.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
Revised R5.1	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
Original R6	The Responsible Entity has established but not documented either a change control or configuration management process.	The Responsible Entity has established but not documented a change control and configuration management process.	The Responsible Entity has not established nor documented either a change control or configuration management process.	The Responsible Entity has not established nor documented a change control and configuration management process.
Revised R6	The Responsible Entity has established but not documented a change control process	The Responsible Entity has established but not documented both a change control process and	The Responsible Entity has not established and documented a change control process	The Responsible Entity has not established and documented a change control process

Summary of Changes Made to VSLs for CIP-003-1 Security Management Controls				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>OR</p> <p>The Responsible Entity has established but not documented a configuration management process.</p>	<p>configuration management process.</p>	<p>OR</p> <p>The Responsible Entity has not established and documented a configuration management process.</p>	<p>AND</p> <p>The Responsible Entity has not established and documented a configuration management process.</p>

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<i>Comment: The VSLs are determined w/o regard to any of the subrequirements, which they should.</i>			
<b>Response:</b> Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.					
Tampa Electric	R1	<i>Comment: The VSLs under requirement 1, do not make sense. It is a higher VSL to have missed a single requirement from CIP002 through CIP009 or to not have the policy readily available to all personnel than it is to not have implemented a cyber security policy at all??? We do not believe this should be a VSL, as the actual violation should be related to the individual requirements that are not met. If it is a violation then it surely belongs at a lower severity level than not having a policy at all.</i>			
<b>Response:</b> Each requirement must be considered by itself when assigning VSLs. Requirement R1 addresses only the existence or non-existence of a policy, not its content.					
IRC SRC, IESO	R1.1	<i>Comment: Binary: OK, and hence should form the basis for determining the VSL for R1.</i>			
<b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.					
SoCal	R1.1	The Responsible Entity's cyber security policy does address all the requirements in Standards CIP-002 through CIP-009, however, it does not include provision for emergency situations.	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, nor does it include provision for emergency situations.	N/A	N/A
<b>Response:</b> The suggested modifications were not adopted. Where a requirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.					

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Tampa Electric	R1.1	<i>Comment: The VSLs under requirement 1, do not make sense. It is a higher VSL to have missed a single requirement from CIP002 through CIP009 or to not have the policy readily available to all personnel than it is to not have implemented a cyber security policy at all.</i>			
<p><b>Response:</b> Each requirement must be considered by itself when assigning VSLs. Requirement R1 addresses only the existence or non-existence of a policy, not its content.</p>					
IRC SRC, IESO	R1.2	<i>Comment: Binary: OK, and hence should form the basis for determining the VSL for R1.</i>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
SoCal	R1.2			The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	<del>The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.</del>
<p><b>Response:</b> The suggestion to move the VSL for noncompliance with this binary subrequirement from Severe to High was not adopted. Noncompliance with a binary subrequirement is always Severe.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Tampa Electric	R1.2	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.			
<p><b>Response:</b> The suggestion to move the VSL for noncompliance with this binary subrequirement from Severe to Lower was not adopted. Noncompliance with a binary subrequirement is always Severe.</p>					
IRC SRC, IESO	R1.3	<p><i>Comment: Not binary. In itself OK. These VSLs can also form the basis for determining the VSL for R1.</i></p>			
<p><b>Response:</b> Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
Tampa Electric	R1.3	The Responsible Entity's senior manager, assigned pursuant to R2, annually reviewed but did not annually approve its cyber security policy.	he		
<p><b>Response:</b> The suggestion to move the High VSL to Lower was not adopted. A failure to approve the cyber security policy is a significant aspect of this subrequirement, and since there are only two aspects to this subrequirement, this is a High VSL, not a Lower VSL.</p>					
IRC SRC, IESO	R2	<p><i>Comment: The VSL should be graded according to how many of R2.1 to R2.3 are missed.</i></p>			
<p><b>Response:</b> Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
Tampa Electric	R2	<p><i>Comment - Not identifying the senior manager by name title and address is the same VSL as not having a senior manager at all? Not updating the information within 30 days is also severe. These are documentation issues that should be Lower VSLs.</i></p>			

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> As defined, a VSL is an after the fact look at how well the responsible entity met the intent of the requirement. This is quite different from a violation risk factor which determines (if the requirement were to be violated) what would be the impact to the reliability of the bulk electric system. In assigning VSLs it is assumed that the requirement has been violated and the question that remains is how severely the intent of the requirement has been missed. For example if the requirement states that X must be documented and the responsible entity has not documented X then the intent of the requirement has been missed and therefore the severity level must be severe. Similar conditions apply to any and all requirements that are binary in nature (i.e. the requirement is either met or not met) in that not meeting the requirement can only be a severe violation level. The impact on the BES would be taken care of by the violation risk factor; a documentation type of requirement would likely have a lower risk factor than a requirement for specific action (by the responsible entity) that impacts on the BES.</p>					
IRC SRC, IESO	R2.1	<p><i>Comment: OK as a condition to determine R2, but itself can be graded according to which elements are missing.</i></p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
SoCal	R2.1		The senior manager is not identified by one of the following; name, title, business phone, business address, and date of designation.	The senior manager is not identified by name, title, business phone, business address, and date of designation.	<del>The senior manager is not identified by name, title, business phone, business address, and date of designation.</del>
<p><b>Response:</b> The drafting team modified the VSLs for R2.1 so there are proposed VSLs for Moderate, High as suggested, but the drafting team retained the Severe VSL for the situation where all the required elements are missing.</p>					
Tampa Electric	R2.1	The senior manager is not identified by name, title, business phone, business address, and date of designation.			
<p><b>Response:</b> The suggestion to move the High VSL to Lower was not adopted. Suggestions made by other stakeholders proposed alternate VSLs based on partial compliance and these suggestions were adopted so that for R2.1 there are proposed VSLs for Moderate, High and Severe.</p>					

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R2.2	<i>Comment: OK as a condition to determine R2, but itself can be graded according to how late the document is issued.</i>			
<b>Response: Thank you for your positive comment. Based on comments from you and other stakeholders, the drafting team changed its binary approach to a graded approach such that there are four VSLs for noncompliance based on the number of days the change was late.</b>					
SoCal	R2.2			Changes to the senior manager were documented but not within thirty calendar days of the effective date.	Changes to the senior manager were not documented within thirty calendar days of the effective date.
<b>Response: Based on comments from you and other stakeholders, the drafting team changed its binary approach to a graded approach such that there are four VSLs for noncompliance based on the number of days the change was late.</b>					
Tampa Electric	R2.2	Changes to the senior manager were not documented within thirty calendar days of the effective date.			
<b>Response: Based on comments from you and other stakeholders, the drafting team changed its binary approach to a graded approach such that there are four VSLs for noncompliance based on the number of days the change was late.</b>					
IRC SRC, IESO	R2.3	<i>Comment: OK as a condition to determine R2, but itself can be graded since there are two conditions in this subrequirement.</i>			
<b>Response: Thank you for your positive comment. The drafting team thinks it would be impossible to measure the situation where the Senior Manager authorized but didn't document an exception. The measure for this requirement is the "document."</b>					
SoCal	R2.3			The senior manager or delegate(s) authorized exception to the Cyber Security Policy but did not document exception within thirty days.	
<b>Response: The suggestion VSL expands on the subrequirement which does not have any timing component.</b>					

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R3	<i>Comment: It doesn't make sense that the Low and Moderate entries are assigned N/A when the VSLs can be further graded to capture the conditions where the responsible entity fails to meet any of R3.1 to R3.3.</i>			
<b>Response: Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
IRC SRC, IESO	R3.1 – R3.3	<i>Comment: The VSLs for this and the other two subrequirements seem OK, but it illustrates the inconsistent approach between R2 and R3. The VSLs for R2's subrequirements should be graded in a similar fashion.</i>			
<b>Response: Where there were specific suggestions to add more gradations to the VSLs for the subrequirements in R2, the drafting team adopted these suggestions. Please see the additional VSLs that were added to R2.1 and R2.2.</b>					
SoCal	R3.2			The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary  OR  The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but the exception did not include compensating measures or a statement accepting risk.	The Responsible Entity has a documented exception to the cyber security policy (pertaining to CIP 002 through CIP 009) but did not include an explanation as to why the exception is necessary, nor did it include any compensating measures or a statement accepting risk.
<b>Response: The suggestion to reformat the VSLs for High and Severe was adopted.</b>					
IRC SRC, IESO	R4	<i>Comment: OK, given the nature of the main and subrequirements and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R4's VSLs according to the extent to which the responsible entity fails to meet its subrequirements.</i>			

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
SoCal	R4			The Responsible Entity documented but did not implement a program to identify, classify, and protect information associated with Critical Cyber Assets.	
<p><b>Response:</b> The suggestion to rephrase the High VSL was adopted.</p>					
IRC SRC, IESO	R4.1	<p><i>Comment: The VSL starts off at the High level for missing one of the elements. This should be Low. Missing 2 a Moderate, 3 a High, etc.</i></p>			
<p><b>Response:</b> VSLs categorize various degrees of noncompliant performance. If the noncompliant performance is missing a minor element such that the performance measured significantly meets the intent of the requirement, then a Lower VSL is appropriate – In this case, the drafting team believes that all of the elements are significant, and missing even one element severely diminishes the value of the performance in meeting the reliability-related intent of the requirement and thus meets the criteria for a “High” VSL.</p>					
IRC SRC, IESO	R4.2	<p><i>Comment: The VSL could be graded according to the percentage of information that is not classified.</i></p>			
<p><b>Response:</b> It would be very difficult to assess the percentage of information that was not classified, so this suggestion was not adopted.</p>					
IRC SRC, IESO	R4.3	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
IRC SRC, IESO	R5	<p><i>Comment: OK given the way the main and subrequirements are written and the fact that separate VRFs are assigned to them. A more appropriate approach would be to grade R5’s VSLs according to the extent to which the responsible entity fails to meet the subrequirements.</i></p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R5			The Responsible Entity documented but did not implement a program for managing access to protected Critical Cyber Asset information.	
<b>Response: The suggestion to rephrase the High VSL was adopted.</b>					
IRC SRC, IESO	R5.1	<i>Comment: The VSL for R5.1 should be graded according to the extent of failure to meet R5.1.1 and R5.1.2 since they are the conditions for fully meeting R5.1.</i>			
<b>Response: Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R5.1			The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	
<b>Response: The suggestion to add a High VSL for meeting one but not both elements of the requirement was adopted.</b>					
IRC SRC, IESO	R5.1.1	<i>Comment: Should be graded since there are a number of elements in this subrequirement.</i>			
<b>Response: There are two VSLs for R5.1.1. The drafting team could not identify noncompliant performance that would meet the criteria for a Lower or Moderate VSL.</b>					
SoCal	R5.1.1		The Responsible Entity did identify the personnel by name, title, business phone but did not identify the information for which they are responsible for authorizing access.	The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.	<del>The Responsible Entity did not identify the personnel by name, title, business phone nor the information for which they are responsible for authorizing access.</del>

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> The suggested revisions were not adopted. Where a requirement has performance that can be graded, there must be a Severe VSL for the situation where the entity's performance is either mostly or fully noncompliant.</p>					
IRC SRC, IESO	R5.1.2	<p><i>Comment: Should be graded according to the delay in verifying the information. Should be graded according to the delay in completing the review.</i></p>			
<p><b>Response:</b> The drafting team continues to believe that this subrequirement is binary – either the information was verified within the specified timeframe or it wasn't.</p>					
SoCal	R5.1.2			The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.	<del>The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.</del>
<p><b>Response:</b> The suggestion to move the VSL for this binary sub-subrequirement to High was not adopted as noncompliance with a binary requirement or subrequirement must be Severe.</p>					
IRC SRC, IESO	R5.2	<p><i>Comment: Should be graded according to the delay in completing the review.</i></p>			
<p><b>Response:</b> The drafting team continues to believe that this subrequirement is binary – either the review was completed within the specified timeframe or it wasn't.</p>					
SoCal	R5.2			The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles	<del>The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles</del>

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
				and responsibilities.	and responsibilities.
<p><b>Response: The suggestion to move the VSL for this binary subrequirement to High was not adopted as noncompliance with a binary requirement or subrequirement must be Severe.</b></p>					
IRC SRC, IESO	R5.3	<p><i>Comment: Should be graded according to the delay in assessing and documenting the processes.</i></p>			
<p><b>Response: The drafting team continues to believe that this subrequirement is binary – either the assessment was completed within the specified timeframe or it wasn't.</b></p>					
SoCal	R5.3			The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.	<del>The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.</del>
<p><b>Response: The suggestion to move the VSL for this binary subrequirement to High was not adopted as noncompliance with a binary requirement or subrequirement must be Severe.</b></p>					
IRC SRC, IESO	R6	<p><i>Comment: OK</i></p>			
<p><b>Response: Thank you for your positive comment.</b></p>					
Tampa Electric	R6	<p><i>Comment: The wording of these levels is very difficult to follow. It appears as though essentially the same violation is both high and severe.</i></p>			
		The Responsible Entity has established but not documented a change control process or: <b>The Responsible Entity has established but not documented</b> a configuration management process.	The Responsible Entity has established but not documented <b>both</b> a change control process and configuration management process.	The Responsible Entity has not established <b>and</b> documented a change control process or : <b>The Responsible Entity has not established and documented</b> a configuration management process. ( <b>what if they documented but did not implement</b> )	The Responsible Entity has not established <b>and</b> documented a change control process and: <b>The Responsible Entity has not established and documented</b> a configuration management process.

All Changes Proposed by Stakeholders for VSLs for CIP-003-1 Security Management Controls					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<b>Response:</b> The drafting team adopted the proposed changes to all four of the VSLs as they add clarity.					

**CIP-004-1 Personnel and Training**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-004-1. The drafting team adopted several of the proposed modifications. All changes made to the VSLs were made based on stakeholder comments and are shown in the first table – and the modifications that were proposed by stakeholders are shown in the second table below.

Summary of Changes Made to VSLs for CIP-004-1 Personnel and Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R1	The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did document but did not establish (implement), nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not establish (implement), maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
Revised R1.	The Responsible Entity established and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	<b>The Responsible Entity established and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.</b>  <b>AND</b>  The Responsible Entity did not	The Responsible Entity did document but did not <b>establish nor maintain</b> a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	The Responsible Entity did not <b>establish, maintain, nor document</b> a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.

Summary of Changes Made to VSLs for CIP-004-1 Personnel and Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		provide security awareness reinforcement on at least a quarterly basis.		
Original R2	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsibility Entity did not review the training program on an annual basis.	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
Revised R2	The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	<p>The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets</p> <p>AND</p> <p>The Responsible Entity did not review the training program on an annual basis.</p>	The Responsible Entity did document but did not establish nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.	The Responsible Entity did not establish, maintain, nor document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
Original R2.2	N/A	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.

Summary of Changes Made to VSLs for CIP-004-1 Personnel and Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Revised R2.2	N/A	The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
Original R3	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access, but the program is not documented.	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in sixty (60) days or more of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.  OR  The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.
Revised R3	N/A	The Responsible Entity has a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in more than thirty (30) days of such personnel being granted such access.	The Responsible Entity does not have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized

Summary of Changes Made to VSLs for CIP-004-1 Personnel and Training				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
		unescorted physical access, but the program is not documented.		unescorted physical access.  OR  The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access.

All Changes Proposed by Stakeholders for VSLs for CIP-004-1 Personnel and Training					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Tampa Electric	All	<i>Comment: The VSLs for this particular standard appear to take into account the relative severity of the violation much better than the other VSLs in the document. Thought was definitely given to the extent to which the requirement was violated. We recommend that consideration be given to the other sections in this same manner.</i>			
<b>Response: The drafting team thanks you for your positive comment – the team made its best effort at applying the criteria for assigning VSLs to all the requirements in all the standards associated with this project.</b>					
IRC SRC, IESO	R1	<i>Comment: OK, but could be improved to consider inclusion of the bulleted elements.</i>			
<b>Response: Because the bulleted items are not “required” but instead are examples, the drafting team did not modify the VSLs to reference the bulleted items.</b>					
NPCC	R1	Remove “(implementation)”	Remove “(implementation)”	Remove “(implementation)”	Remove “(implementation)”
<b>Response: Agreed – the word, “implement” was not part of the requirement and has been removed from the VSLs for R1.</b>					
SoCal	R1		The Responsible Entity established (implemented), and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. And did not provide security awareness reinforcement on at least a quarterly basis.		
<b>Response: The proposed expansion of the Moderate VSL was adopted.</b>					
IRC SRC, IESO	R2	<i>Comment: OK given the current structure and assignment of VRFs to R2 and its subrequirements.</i>			

All Changes Proposed by Stakeholders for VSLs for CIP-004-1 Personnel and Training					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<b>Response: Thank you for your positive comment.</b>					
SoCal	R2		The Responsible Entity established and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets and did not review the training program on an annual basis.		
<b>Response: The proposed expansion of the Moderate VSL was adopted.</b>					
IRC SRC, IESO	R2.1	<i>Comment: OK</i>			
<b>Response: Thank you for your positive comment.</b>					
IRC SRC, IESO	R2.2	<i>Comment: Could be improved to stipulate conditions for Low and Moderate since the requirement itself contains several conditions: "...policies, access controls, and procedures". None of them are covered in the High and Severe VSLs.</i>			
<b>Response: The key elements of this subrequirement are the topics listed in the sub-subrequirements. Note that based on a suggestion from other stakeholders, the team did add a Moderate VSL.</b>					
SoCal	R2.2		The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.	The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
<b>Response: The proposed revisions add more levels of VSLs and still support the criteria for assigning VSLs and were adopted.</b>					
IRC SRC, IESO	R2.3	<i>Comment: OK.</i>			
<b>Response: Thank you for your positive comment.</b>					

All Changes Proposed by Stakeholders for VSLs for CIP-004-1 Personnel and Training					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R2.3		The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.	<del>The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records.</del>
<p><b>Response: Shifting the VSLs so there are only Moderate and High VSLs was not adopted. Total noncompliance must always be a Severe VSL. If the training records don't contain the names of those who participated or the date, then the entity hasn't met a significant element of the subrequirement to the extent that the entity can't demonstrate that all personnel who should have received the training were trained – this is significant enough to warrant a High VSL.</b></p>					
IRC SRC, IESO	R3	<p><i>Comment: OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i></p>			
<p><b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b></p>					
SoCal	R3			The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program in thirty (30) days of such personnel being granted such access.	
<p><b>Response: The drafting team adopted your suggestion that a timing component be added to the range of noncompliant performance associated with a High VSL.</b></p>					
IRC SRC, IESO	R3.1-R3.3	<p><i>Comment: OK</i></p>			
<p><b>Response: Thank you for your positive comment.</b></p>					
IRC SRC, IESO	R4	<p><i>Comment: OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i></p>			

All Changes Proposed by Stakeholders for VSLs for CIP-004-1 Personnel and Training					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO, IESO	R4.1-R4.2	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
Duke Energy	R4.2			N/A	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.
<p><b>Response:</b> The drafting team did not adopt this suggested revision to the Severe VSL. A Severe violation should reflect failure to meet both elements of this requirement. The failure to revoke access to Critical Cyber Assets within 24 hours is a failure to meet a significant part of the requirement, which meets the criteria for assignment of a High VSL.</p>					

**CIP-005-1 Electronic Security Perimeter(s)**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-005-1. The drafting team adopted several of the proposed modifications and corrected a typographical error. All changes made to the VSLs were made based on stakeholder comments (except for the typographical error) and are shown in the first table – and the modifications that were proposed by stakeholders are shown in the second table below.

Summary of Changes Made to VSLs for CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R1	The Responsible Entity did not document one or more access points to the electronic security perimeter(s).	The Responsible Entity did not identify and document all Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.	The Responsible Entity did not ensure that one or more Critical Cyber Asset resides within an Electronic Security Perimeter, and the Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.
Revised R1.	The Responsible Entity did not document one or more access points to the electronic security perimeter(s).	The Responsible Entity <b>identified but</b> did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.  <b>OR</b>  The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Assets resides within an Electronic Security Perimeter.  <b>AND</b>  The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s) for all Critical Cyber Assets.

Summary of Changes Made to VSLs for CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R2.4	N/A	N/A	N/A	The Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
Revised R2.4	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
Original R2.6	The Responsible Entity did not maintain a document identifying the content of the banner.  OR  Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Summary of Changes Made to VSLs for CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Revised R2.6	<p>The Responsible Entity did not maintain a document identifying the content of the banner.</p> <p>OR</p> <p>Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>	<p>Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.</p>
Original R3.1	<p>The Responsible Entity did not document the electronic or manual processes for monitoring and logging access points to dial-up devices.</p> <p>OR</p> <p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes monitoring and logging at less than 5% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 5% or more but less than 10% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 10% or more but less than 15% of the access points to dial-up devices.</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring and logging at 15% or more of the access points to dial-up devices.</p>
Revised R3.1	<p>The Responsible Entity did not document the electronic or manual processes for monitoring access</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual</p>	<p>Where technically feasible, the Responsible Entity did not implement electronic or manual</p>

Summary of Changes Made to VSLs for CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
	<p>points to dial-up devices.</p> <p>OR</p> <p>Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at less than 5% of the access points to dial-up devices.</p>	<p>processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.</p>	<p>processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.</p>	<p>processes for monitoring at 15% or more of the access points to dial-up devices.</p>
Original R4	<p>The Responsible Entity performed at least annually a Vulnerability Assessment for more than 95% but less than 100% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity performed at least annually a Vulnerability Assessment for more than 90% but less than or equal to 95% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity performed at least annually a Vulnerability Assessment for more than 85% but less than or equal to 90% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity performed at least annually a Vulnerability Assessment for 85% or less of access points to the Electronic Security Perimeter(s).</p> <p>OR</p> <p>The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R4.5.</p>
Revised R4	<p>The Responsible Entity did not perform a Vulnerability Assessment at least annually for less than 5% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not perform a Vulnerability Assessment at least annually for 5% or more but less than 10% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not perform a Vulnerability Assessment at least annually for 10% or more but less than 15% of access points to the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not perform a Vulnerability Assessment at least annually for 15% or more of access points to the Electronic Security Perimeter(s).</p>

Summary of Changes Made to VSLs for CIP-005-1 Electronic Security Perimeter(s)				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR  The vulnerability assessment did not include one (1) or more of the subrequirements R 4.1, R4.2, R4.3, R4.4, R45.
Original R5.3	N/A	N/A	N/A	The responsible Entity did not retain electronic access logs for at least 90 calendar days.
Revised R5.3	The Responsible Entity did not retain electronic access logs for at least 90 calendar days.	The Responsible Entity retained electronic access logs for more than 90 but less than 120 calendar days.	The responsible Entity retained electronic access logs for 120 calendar days or more but less than 150 calendar days.	The responsible Entity did not retain electronic access logs.

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO, IESO	R1	<i>Comment: OK given the current structure and assignment of VRFs to R1 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R1	The Responsible Entity did not document one or more access points to the electronic security perimeter(s).	The Responsible Entity identified but did not document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more of the Critical Cyber Assets resides within an Electronic Security Perimeter.  OR  The Responsible Entity did not identify nor document one or more Electronic Security Perimeter(s).	The Responsible Entity did not ensure that one or more Critical Cyber Asset resides within an Electronic Security Perimeter, AND the Responsible Entity did not identify and document one or more Electronic Security Perimeter(s)
<p><b>Response: The alternate Lower VSL that was proposed is identical to the Lower VSL that was proposed by the drafting team. The team adopted the proposed alternative for the Moderate and High VSLs. The team did not adopt the suggested modification for the Severe VSL as this would have omitted failure to identify access points to the perimeter(s) for all Critical Cyber Assets.</b></p>					
IRC SRC, IESO, IESO	R1.1- R1.6	<i>Comment: OK</i>			
<p><b>Response: Thank you for your positive comment</b></p>					
NPCC	R1.1	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"	Remove "(for example dial-up modem)"
<p><b>Response: The drafting team did not adopt the suggested change to the VSLs. The parenthetical phrase was in the requirement and the language in the VSLs should be consistent with the wording of the requirement.</b></p>					
SoCal	R1.1			Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	<del>Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).</del>

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> The suggested modification was not adopted. Where a requirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.</p>					
Tampa Electric	R1.1	Documentation of access points to the Electronic Security Perimeter(s) do not include all externally connected communication end points (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).			Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end points (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s), and such access points have not been protected.
<p><b>Response:</b> The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</p>					
Tampa Electric	R1.1 – R1.3	Comment: The VSLs for these violations should vary depending upon the severity of the actual violation. Mis-documenting the access points should not be severe. Not documenting <b>and</b> protecting access points should be.			
<p><b>Response:</b> VSLs do not assess the severity of a violation on reliability. Violation Risk Factors (VRFs) assess the impact the violation of a requirement may have on reliability. VSLs are categories of noncompliant performance, ranging from nearly compliant to mostly or totally noncompliant.</p>					
SoCal	R1.2			For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.	For more than two (2) dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic Security Perimeter for that single access point at the dial-up device.
<p><b>Response:</b> The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Tampa Electric	R1.2	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity created by did not document an Electronic Security Perimeter for that single access point at the dial-up device.			For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not create an Electronic Security Perimeter for that single access point at the dial-up device.
<p><b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b></p>					
SoCal	R1.3			At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.	At least one end point of a communication link within the <del>Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.</del>
<p><b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b></p>					
Tampa Electric	R1.3	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was protected as but not documented as an access point to the Electronic Security Perimeter.			At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not protected as an access point to the Electronic Security Perimeter.
<p><b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b></p>					

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R1.4	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified but is protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is identified but not protected pursuant to the requirements of Standard CIP-005.	One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.	<del>One or more non-critical Cyber Asset within a defined Electronic Security Perimeter is not identified and is not protected pursuant to the requirements of Standard CIP-005.</del>
<b>Response: The drafting team did not adopt the proposed modifications to shift the VSLs so that there is no Severe VSL. Total noncompliance with a requirement must always be categorized as a Severe VSL.</b>					
SoCal	R1.6		The Responsible Entity did not maintain documentation of one of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access point to the Electronic Security Perimeter(s) or Cyber Asset deployed for the access control and monitoring of these access points.	The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.	<del>The Responsible Entity did not maintain documentation of two or more of the following: Electronic Security Perimeter(s), interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.</del>
<b>Response: The drafting team did not adopt the proposed modifications to shift the VSLs so that there is no Severe VSL. Total noncompliance with a requirement must always be categorized as a Severe VSL.</b>					
IRC SRC, IESO	R2	<i>Comment: OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
SoCal	R2.3		The Responsible Entity has a procedure but not maintained for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not document nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.	The Responsible Entity did not document, implement, nor maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
<p><b>Response:</b> The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graduated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</p>					
IRC SRC, IESO	R2.4-R2.6	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
SoCal	R2.4				Where external interactive access into the Electronic Security Perimeter has been enabled. the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
<p><b>Response:</b> The drafting team adopted your suggested additional language for the Severe VSL as this improves the VSL’s clarity.</p>					
Duke Energy	R2.6		Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.		

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> The drafting team adopted your suggested modification to the Moderate VSL as this eliminates the duplication between the Moderate and High VSLs that existed in the set of VSLs that was posted for stakeholder review.</p>					
SoCal	R2.6		Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.		
<p><b>Response:</b> The drafting team adopted your suggested modification to the Moderate VSL as this eliminates the duplication between the Moderate and High VSLs that existed in the set of VSLs that was posted for stakeholder review.</p>					
IRC SRC, IESO	R3	<p><i>Comment: OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i></p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R3.1- R3.2	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
SoCal	R3.1	Where technically feasible, the Responsible Entity implemented but did not documented electronic or manual processes monitoring and logging at less than 5% of the access points to dial-up devices.			
<p><b>Response:</b> The suggested language was not adopted. The VSLs must recognize if the responsible entity has failed to document the electronic or manual processes for monitoring access points.</p>					
Tampa	R3.1	<p><i>Comment: This VSL includes logging in the severity level, but the requirement is only for the establishment of monitoring procedures.</i></p>			

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Electric		<i>Logging is only required under the top level requirement R3. Additionally this should be a lower severity level. By the way, what is a manual logging process for electronic access points, and how could that be an effective control?</i>			
		The Responsible Entity did not document the electronic or manual processes for monitoring access points to dial-up devices.  OR  Where technically feasible, the Responsible Entity did not implement electronic or manual processes monitoring at less than 5% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 5% or more but less than 10% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 10% or more but less than 15% of the access points to dial-up devices.	Where technically feasible, the Responsible Entity did not implement electronic or manual processes for monitoring at 15% or more of the access points to dial-up devices.
<b>Response: The drafting team adopted your suggestions and removed the phrase, “and logging” from all four VSLs as the phrase, “and logging” is not part of the subrequirement.</b>					
IRC SRC, IESO	R4	<i>Comment: OK for the conditions that are independent of R4.1 to R4.4. Assigning a Severe VSL for missing any one (or more) of R4.1 to R4.4 is like treating it a like binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.</i>			
<b>Response: Thank you for your positive comment. The drafting team changed the VSLs so they use percentages to categorize degrees of noncompliant performance.</b>					
Tampa Electric	R4	<i>Comment: This VSL departs from the measurements used for other similar VSLs. For consistency this should use the 5%, 10%, 15% measurements as used in the other VSLs.</i>			
<b>Response: The drafting team changed the VSLs so they use percentages to categorize degrees of noncompliant performance.</b>					
NPCC	R4 and others	VSLs should identify what has not been demonstrated as the Standard calls for. Request that the percentage thresholds be consistent, as in the earlier Requirements that use percentages.			

All Changes Proposed by Stakeholders for VSLs for CIP-005-1 Electronic Security Perimeter(s)					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> The drafting team changed the VSLs so they use percentages to categorize degrees of noncompliant performance. The team only made this modification for the R4 VSLs as this was the only set of VSLs where this seemed applicable.</p>					
IRC SRC, IESO	R5	<p><i>Comment: OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i></p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R5.1-R5.2	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
IRC SRC, IESO	R5.3	<p><i>Comment: Should be graded according to the number of days that the log was maintained.</i></p>			
<p><b>Response:</b> Based on your comments and the comments of others, the drafting team revised the VSLs so they offer four categorizes of noncompliant performance based on the number of days the access logs were retained.</p>					
SoCal	R5.3			The responsible Entity did not retain electronic access logs for at least 90 calendar days.	<del>The responsible Entity did not retain electronic access logs for at least 90 calendar days.</del>
<p><b>Response:</b> Based on your comments and the comments of others, the drafting team revised the VSLs so they offer four categorizes of noncompliant performance based on the number of days the access logs were retained.</p>					
Tampa Electric	R5.3	<p><i>Comment: There should be varying levels of severity with this requirement. For example if an entity is missing 1 hour of access logs or one day, or all access logs the VSL is the same. Consideration also needs to be given to the number of access points for which logging must take place and the possibility that a server hardware or software failure could result in lost log data. Did a technical problem (hardware error) occur, human error, an implementation oversight, or ignorance of the requirement? These are all factors that should weigh into the severity level.</i></p>			
<p><b>Response:</b> Based on your comments and the comments of others, the drafting team revised the VSLs so they offer four categorizes of noncompliant performance based on the number of days the access logs were retained.</p>					

**CIP-006-1 Critical Cyber Assets**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-006-1. The drafting team adopted a suggestion to modify the VSLs for Requirement R5 to provide more categories for noncompliant performance. The sole change made to the VSLs was made based on stakeholder comments and is shown in the first table – and the modifications that were proposed by stakeholders are shown in the second table below.

Summary of Changes Made to VSLs for CIP-006-1 Physical Security of Critical Cyber Assets				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R5	N/A	N/A	N/A	The Responsible Entity did not retain electronic access logs for at least ninety calendar days.
Revised R5	The Responsible Entity did not retain electronic access logs for at least 90 calendar days.	The Responsible Entity did not retain electronic access logs for 120 calendar days or more but less than 150 calendar days.	The Responsible Entity retained electronic access logs for more than 90 but less than 120 calendar days.	The Responsible Entity did not retain electronic access logs.

All Changes Proposed by Stakeholders for VSLs for CIP-006-1 Physical Security of Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<i>Comment: The VSLs for R1 should be determined according to the extent of failure to meet any of its subrequirements this requirement, as it is so clearly indicated in R1 that the plan shall address, at a minimum, the subrequirements that follow.</i>			
<b>Response: Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R1.1			The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets	

All Changes Proposed by Stakeholders for VSLs for CIP-006-1 Physical Security of Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
				within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter.  OR  Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity has not deployed nor documented alternative measures to control physical access to the Critical Cyber Assets.	
<b>Response:</b> The suggested modification was not adopted. Where a subrequirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.					
IRC SRC, IESO	R1.1, R1.2, R1.4-R1.9	<i>Comment: OK</i>			
<b>Response:</b> Thank you for your positive comment.					
IRC SRC, IESO	R1.3	<i>Comment: OK as a condition to determine the VSL for R1 but since it is not, the VSLs for R1.3 should be graded according to which element among “processes, tools, and procedures” is missing.</i>			
<b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.					
SoCal	R1.7		The Responsible Entity's physical security plan includes a process for updating the physical security plan within ninety calendar days of any physical security system	The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system redesign or	<del>The Responsible Entity's physical security plan does not include a process for updating the physical security plan within ninety calendar days of any physical security system</del>

Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels

All Changes Proposed by Stakeholders for VSLs for CIP-006-1 Physical Security of Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
			redesign or reconfiguration <del>but</del> the plan was not updated within 90 calendar days of any physical security system redesign or reconfiguration.	reconfiguration.	<del>redesign or reconfiguration.</del>
<p><b>Response:</b> The suggested modification was not adopted. Where a subrequirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.</p>					
<p><b>Response:</b></p>					
IRC SRC, IESO	R2	<p><i>Comment:</i> OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R3	<p><i>Comment:</i> OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R4	<p><i>Comment:</i> OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R5	<p>Should be graded according to the number of days that the log was maintained.</p>			
<p><b>Response:</b> The drafting team modified the VSLs so they are graded based on the number of days the log was not retained.</p>					
SoCal	R5			The Responsible Entity did not retain electronic access logs for at least ninety calendar days.	<del>The Responsible Entity did not retain electronic access logs for at least ninety calendar days.</del>
<p><b>Response:</b> The drafting team modified the VSLs so they are graded based on the number of days the log was not retained.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-006-1 Physical Security of Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
Tampa Electric	R5	Comment: There should be varying levels of severity with this requirement. For example if an entity is missing 1 hour of access logs or one day, or all access logs the VSL is the same. Consideration needs to be given to the number of access points for which logging must take place and the possibility that a server hardware or software failure could result in lost log data. Did a technical problem occur, human error, an implementation oversight, or ignorance of the requirement? These are all factors that should weigh into the severity level.			
				The responsible entity did not retain logs for at least 90 calendar days.	The responsible entity did not retain logs.
<p><b>Response: The drafting team modified the VSLs so they are graded based on the number of days the log was not retained.</b></p>					
IRC SRC, IESO	R6	<p><i>Comment:</i> OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</p>			
<p><b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b></p>					

**CIP-007-1 Systems Security Management**

**Summary Consideration:** There were several suggestions for modifications to the originally proposed VSLs for CIP-007-1. The drafting team adopted several of the proposed modifications. All changes made to the VSLs were made based on stakeholder comments and are shown in the first table – and the modifications that were proposed by stakeholders are shown in the second table below.

Summary of Changes Made to VSLs for CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Original R1.	N/A	<p>The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, <b>but did not document</b> that testing is performed as required in R1.2.</p> <p>OR</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>	<p>The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.</p>	<p>The Responsible Entity <b>did not create, implement nor maintain</b> the test procedures as required in R1.1, did not document that testing is performed as required in R1.2, and did not document the test results as required in R1.3.</p>
Revised R1.	N/A	<p>The Responsible Entity did create, implement and maintain the test procedures as required in R1.1, <b>but did not document</b> that testing is performed as required in R1.2.</p> <p>OR</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>	<p>The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1.</p>	<p>The Responsible Entity did not create, implement <b>and</b> maintain the test procedures as required in R1.1,</p> <p><b>AND</b></p> <p><b>The Responsible Entity</b> did not document that testing was performed as required in R1.2</p>

Summary of Changes Made to VSLs for CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				<p>AND</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>
Original R3.2	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of applicable security patches as required in R3.</p> <p>OR</p> <p>Where the applicable patch is not installed, the Responsible Entity did not document the implementation of the patch or compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.</p>
Revised R3.2.	N/A	N/A	N/A	<p>The Responsible Entity did not document the implementation of applicable security patches as required in R3.</p> <p>OR</p> <p>Where an applicable patch was not</p>

Summary of Changes Made to VSLs for CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
				installed, the Responsible Entity <b>did not document the compensating measure(s)</b> applied to mitigate risk exposure or an acceptance of risk.
Original R4.	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
Revised R4.	The Responsible Entity, <b>as technically feasible</b> , did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, <b>as technically feasible</b> , did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, <b>as technically feasible</b> , did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, <b>as technically feasible</b> , did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
Original R4.2	The Responsible Entity documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing of the signatures.	The Responsible Entity <b>did not document but implemented</b> a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity <b>documented but did not implement</b> a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity <b>did not document nor implement</b> a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”

Summary of Changes Made to VSLs for CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Revised R4.2	The Responsible Entity, as <b>technically feasible</b> , documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing and <b>installation</b> of the signatures.	The Responsible Entity, as <b>technically feasible, did not document but implemented</b> a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as <b>technically feasible, documented but did not implement</b> a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	The Responsible Entity, as <b>technically feasible, did not document nor implement</b> a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
Original R5	The Responsible Entity <b>did not document but implemented</b> technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented and implemented technical and procedural controls that enforce access authentication and accountability, <b>however</b> those technical and procedural controls are not enforced for all user activity.	The Responsible Entity implemented technical and procedural controls that enforce access authentication <b>but</b> does not provided accountability for, all user activity.	The Responsible Entity <b>did not document nor implement</b> technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
Revised R5.	<del>The Responsible Entity <b>did not document but implemented</b> technical and procedural controls that enforce access authentication of, and accountability for, all user activity.</del> <a href="#">NA</a>	The Responsible Entity implemented but did not document technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity documented but did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity did not document nor implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
Original R5.3	The Responsible Entity requires and uses passwords but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity <b>requires but does not use passwords</b> as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity <b>does not require nor use passwords</b> as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.

Summary of Changes Made to VSLs for CIP-007-1 Systems Security Management				
R#	Lower VSL	Moderate VSL	High VSL	Severe VSL
Revised R5.3	The Responsible Entity requires and uses passwords <b>as technically feasible</b> , but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords <b>as technically feasible</b> but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity <b>requires but does not use passwords</b> as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.	The Responsible Entity <b>does not require nor use passwords</b> as required in R5.3.1, R5.3.2., R5.3.3 and did not demonstrate why it is not technically feasible.
Original R9	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>or</b> the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>nor</b> were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.
Revised R9	The Responsible Entity did review and update the documentation specified in Standard CIP-007 at least annually <b>but</b> the Responsible Entity did not document changes resulting from modifications to the systems or controls within 90 calendar days of the changes to the systems or controls.	The Responsible Entity did review and update the documentation specified in Standard CIP-007 at least annually <b>but</b> the Responsible Entity did not document Changes resulting from modifications to the systems or controls for 90 or more but less than 120 calendar days of the changes to the systems or controls.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>but</b> the Responsible Entity did not document Changes resulting from modifications to the systems or controls <b>for 120 or more but less than 150 calendar days</b> of the changes to the systems or controls.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>AND</b> The Responsible Entity did not document changes resulting from modifications to the systems or controls for <b>150 or more</b> calendar days <b>beyond the date</b> of the changes to the systems or controls.

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<i>Comment: OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R1				<p>The Responsible Entity did not create, implement and maintain the test procedures as required in R1.1,</p> <p>AND</p> <p>The Responsible Entity did not document that testing was performed as required in R1.2</p> <p>AND</p> <p>The Responsible Entity did not document the test results as required in R1.3.</p>
<b>Response: The drafting team adopted your suggested reformatting of the Severe VSL.</b>					
IRC SRC, IESO	R2	<i>Comment: OK given the current structure and assignment of VRFs to R2 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R2	The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are	N/A	N/A	N/A

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
		enabled.			
<p><b>Response:</b> The suggested modification was not adopted. Where a requirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.</p>					
Tampa Electric	R2	<p><i>Comment: For this requirement it would seem to make more sense to focus on whether or not the program was applied to all critical cyber assets and cyber assets within the ESP Levels high and severe are the same net result, but you get credit for having documented something you are not executing. Suggested wording changes below:</i></p>			
		<p>The Responsible Entity established but did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>	<p>The Responsible Entity <b>established</b> a process to ensure that only those ports and services required for normal and emergency operations are enabled, but failed to exercise this process on less than 5% of critical cyber assets.</p>	<p>The Responsible Entity <b>established</b> a process to ensure that only those ports and services required for normal and emergency operations are enabled , but failed to exercise this process on more than 5% of critical cyber assets</p>	<p>The Responsible Entity did not establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.</p>
<p><b>Response:</b> The drafting team did not adopt the proposed revisions. Graded VSLs address varying levels of noncompliance to the intent of a requirement. The fact that an entity has at least documented its process demonstrates “partial-credit” toward compliance with the requirement.</p>					
IRC SRC, IESO	R2,1, R2.2	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
SoCal	R2.2	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for at least one but less than 5% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 5% or more but less than 10% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 10% or more but less than 15% of the Cyber Assets inside the Electronic Security Perimeter(s).</p>	<p>The Responsible Entity did not disable other ports and services, including those used for testing purposes, prior to production use for 15% or more of the Cyber Assets inside the Electronic Security Perimeter(s).</p>
<p><b>Response:</b> The proposed language matches the language that is in the posted version of the VSLs.</p>					

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R2.3	<i>Comment: Should be graded according to the number or % of cases that the responsible entity failed to document compensated measure(s) for those unused ports and services cannot be disabled.</i>			
<b>Response: The drafting team did not adopt this suggestion. There is no way to identify if there will be any cases, or how many cases, may exist, thus developing a set of % that would accurately categorize different degrees of noncompliant performance is not recommended.</b>					
IRC SRC, IESO	R3	<i>Comment: OK given the current structure and assignment of VRFs to R3 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
IRC SRC, IESO	R3.1	<i>Comment: OK</i>			
<b>Response: Thank you for your positive comment.</b>					
IRC SRC, IESO	R3.2	<i>Comment: Should be graded according to the number or % of cases that the responsible entity failed to document the implementation of security patches and/or failed to document compensated measure(s) for those patches that are not installed.</i>			
<b>Response: The drafting team did not adopt this suggestion. There is no way to identify if there will be any cases, or how many cases, may exist, thus developing a set of % that would accurately categorize different degrees of noncompliant performance is not recommended.</b>					
SoCal	R3.2				<p>The Responsible Entity did not document the implementation of applicable security patches as required in R3.</p> <p>OR</p> <p>Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.</p>

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<b>Response: The drafting team adopted the proposed language as it more closely matches the language in the associated requirement.</b>					
IRC SRC, IESO	R4	<i>Comment: OK given the current structure and assignment of VRFs to R4 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
AEP	R4	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least one but less than 5% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 5% but less than 10% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on at least 10% but less than 15% of Cyber Assets within the Electronic Security Perimeter(s).	The Responsible Entity, as technically feasible, did not use anti-virus software and other malicious software (“malware”) prevention tools, nor implemented compensating measures, on 15% or more Cyber Assets within the Electronic Security Perimeter(s).
<b>Response: The drafting team added, “as technically feasible” to each of the VSLs as proposed.</b>					
AEP	R4.1	N/A	N/A	N/A	The Responsible Entity, as technically feasible, did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.  OR  The Responsible Entity, as technically feasible, did not document the implementation of compensating measure(s) applied to mitigate risk

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
					exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.
<b>Response: The drafting team did not adopt this suggestion. The term, “technically feasible” is not used in R4.1.</b>					
IRC SRC, IESO	R4.1	<i>Comment: Should be graded according to the number or % of cases that the responsible entity failed to meet either of the two conditions stipulated in this subrequirements.</i>			
<b>Response: The drafting team did not adopt this suggestion. There is no way to identify if there will be any cases, or how many cases, may exist, thus developing a set of % that would accurately categorize different degrees of noncompliant performance is not recommended.</b>					
SoCal	R4.1			The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.	<del>The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter.</del>  OR  <del>The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure or an acceptance of risk where antivirus and malware prevention tools are not installed.</del>
<b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b>					
AEP	R4.2	The Responsible Entity, as technically feasible, documented and implemented	The Responsible Entity, as technically feasible, <b>did not document but implemented a</b>	The Responsible Entity, as technically feasible, <b>documented but did not implement a</b>	The Responsible Entity, as technically feasible, <b>did not document nor implement a</b>

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
		a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing of the signatures.	process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”	process including addressing testing and installing the signatures for the update of anti-virus and malware prevention “signatures.”
<p><b>Response: The drafting team adopted the suggested modifications and added, “as technically feasible” to each of the VSLs – and added “installation” to the Lower VSL.</b></p>					
IRC SRC, IESO	R4.2	<i>Comment: OK</i>			
<p><b>Response: Thank you for your positive comment.</b></p>					
SoCal	R4.2	The Responsible Entity documented and implemented a process for the update of anti-virus and malware prevention “signatures.”, but the process did not address testing and installing of the signatures.	The Responsible Entity <b>implemented but did not document</b> a process, including addressing testing and installing the signatures, for the update of anti-virus and malware prevention “signatures.”		
<p><b>Response: The drafting team adopted the proposed language for the Lower VSL but not for the Moderate VSL – the proposed language for the Moderate VSL is already in the High VSL.</b></p>					
IRC SRC, IESO	R5	<i>Comment: OK given the current structure and assignment of VRFs to R5 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			
<p><b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b></p>					
SoCal	R5	N/A	The Responsible Entity implemented but <b>did not document</b> technical and procedural controls that enforce access authentication of, and accountability for, all user	The Responsible Entity documented <b>but did not implement</b> technical and procedural controls that enforce access authentication of, and accountability for, all user activity.	The Responsible Entity <b>did not document nor implemented</b> technical and procedural controls that enforce access authentication of, and accountability for, all user

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
			activity.		activity.
<b>Response: The drafting team adopted the proposed modifications for all four VSLs.</b>					
IRC SRC, IESO	R5.1	<i>Comment: Should be graded according to which of R5.1.1 to R5.1.2 are missed since they are the required elements in the policy.</i>			
<b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graded VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each subrequirement and sub-subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R5.1			The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	<del>The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.</del>
<b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graded VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b>					
IRC SRC, IESO	R5.1.1	<i>Comment: OK by itself but it should get rolled up to the determination of VSLs for R5.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
SoCal	R5.1.1	At least one user account but less than 5% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	5 % or more but less than 10% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	10 % or more but less than 15% of user accounts implemented by the Responsible Entity were not approved by designated personnel.	15 % or more of user accounts implemented by the Responsible Entity were not approved by designated personnel.
<b>Response: The suggestion to modify the percentages in the VSLs to make them higher was not adopted. In many cases, there will be a low number of user accounts on CCA systems – anything more than 5% of these small numbers would be too high a margin of error to meet the criteria for</b>					

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<b>anything but a Severe VSL.</b>					
IRC SRC, IESO	R5.1.2	<i>Comment: OK by itself but it should get rolled up to the determination of VSLs for R5.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
IRC SRC, IESO	R5.1.3	<i>Comment: Binary is OK if it was rolled up to the determination of VSLs for R5. Otherwise, the VSLs should be graded according to the delay in completing the annual review.</i>			
<b>Response: Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</b>					
IRC SRC, IESO	R5.2	<i>Comment: Disagree with the binary VSL since to fully meet the intent of R5.2, all of its subrequirements must be complied with. The VSLs for R5.2 should be graded according to the extent of failing to meet any of its subrequirements.</i>			
<b>Response: The drafting team considers the subrequirement, assessed by itself to be binary. Where a requirement or subrequirement is binary, it is not conducive to graded VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b>					
SoCal	R5.2			The Responsible Entity implemented but did not document a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	<del>The Responsible Entity implemented but did not document a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.</del>
<b>Response: The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graded VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</b>					
IRC SRC, IESO	R5.2.1	<i>Comment: OK</i>			
<b>Response: Thank you for your positive comment.</b>					
IRC SRC, IESO	R5.2.2	<i>Comment: Should be graded according to the number or % of the individuals that the responsible entity failed to identify.</i>			

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> There could be a very low number of user accounts on CCA systems and identifying an appropriate number or percentage for various categories of noncompliant performance is not feasible.</p>					
SoCal	R5.2.2	The Responsible Entity did not identify <5% all individuals with access to shared accounts.	The Responsible Entity did not identify between 5-10% all individuals with access to shared accounts.	The Responsible Entity did not identify between 10-15% all individuals with access to shared accounts.	The Responsible Entity did not identify >15% individuals with access to shared accounts.
<p><b>Response:</b> The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graduated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</p>					
IRC SRC, IESO	R5.2.3	<i>Comment: OK</i>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
SoCal	R5.3	The Responsible Entity requires and uses passwords as technically feasible, but only addresses 2 of the requirements in R5.3.1, R5.3.2., R5.3.3.	The Responsible Entity requires and uses passwords as technically feasible but only addresses 1 of the requirements in R5.3.1, R5.3.2., R5.3.3.		
<p><b>Response:</b> The drafting team adopted the proposal to add the phrase, “as technically feasible” to the Lower and Moderate VSLs so that the language in the VSLs more closely matches the language in the associated subrequirement.</p>					
AEP	R5.3.	The Responsible Entity, as technically feasible, requires and uses passwords but only addresses 2 of the requirements in R5.3.1, R5.3.2, R5.3.3.	The Responsible Entity, as technically feasible, requires and uses passwords but only addresses 1 of the requirements in R5.3.1, R5.3.2, R5.3.3.	The Responsible Entity, as technically feasible, <b>requires but does not use passwords</b> as required in R5.3.1, R5.3.2, R5.3.3, and did not demonstrate why it is not technically feasible.	The Responsible Entity, as technically feasible, <b>does not require nor use passwords</b> as required in R5.3.1, R5.3.2, R5.3.3, and did not demonstrate why it is not technically feasible.
<p><b>Response:</b> The drafting team adopted the proposal to add the phrase, “as technically feasible” to the Lower and Moderate VSLs so that the language in the VSLs more closely matches the language in the associated subrequirement.</p>					
IRC SRC, IESO	R6	<i>Comment: OK given the current structure and assignment of VRFs to R6 and its subrequirements, but could be improved to consider failure to meet any of the subrequirements.</i>			

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R6.1 – R6.4	<p><i>Comment: OK</i></p>			
<p><b>Response:</b> Thank you for your positive comment.</p>					
IRC SRC, IESO	R6.5	<p><i>Comment: Should be graded according to the number or % of the logged cases that the responsible entity failed to review and provided records documenting the review.</i></p>			
<p><b>Response:</b> Response: The drafting team did not adopt this suggestion. There is no way to identify if there will be any cases, or how many cases, may exist, thus developing a set of % that would accurately categorize different degrees of noncompliant performance is not recommended.</p>					
SoCal	R6.5			<p>The Responsible Entity reviewed but not documented logs of system events related to cyber security nor maintain records documenting review of logs.</p>	<p><del>The Responsible Entity reviewed but not documented logs of system events related to cyber security nor maintain records documenting review of logs.</del></p>
<p><b>Response:</b> The drafting team considers the subrequirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to gradated VSLs, and a failure to meet the required performance can only be categorized as a “Severe” VSL.</p>					
IRC SRC, IESO	R7	<p><i>Comment: OK as the subrequirements’ violations are “rolled-up” but each of the subrequirements has a VRF, which by FERC’s rule has to have a VSL!</i></p>			
<p><b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.</p>					
IRC SRC, IESO	R8	<p><i>Comment: OK for the conditions that are independent of R8.1 to R8.4. Assigning a Severe VSL for missing any one (or more) of R8.1 to R8.4 is like treating it like a binary requirement where in fact it can be graded according to how many of R4.1 to R4.4 are missed. Suggest to grade this.</i></p>			
<p><b>Response:</b> Thank you for your positive comment. The drafting team felt that missing any one of the subrequirements would result in a product that fell so short in meeting its reliability objective that it met the criteria for a “Severe” VSL.</p>					
IRC SRC, IESO	R9	<p><i>Comment: Should be expanded to make VSLs also dependent on the delay in documenting the modifications.</i></p>			

All Changes Proposed by Stakeholders for VSLs for CIP-007-1 Systems Security Management					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
<b>Response:</b> Thank you for your comment. The VSLs have been modified to address delays in documenting the modifications.					
SoCal	R9		The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>or</b> the Responsible Entity did not document Changes resulting from modifications to the systems or controls within ninety calendar days of the change.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>nor</b> were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.	<del>The Responsible Entity did not review and update the documentation specified in Standard CIP-007 at least annually <b>nor</b> were Changes resulting from modifications to the systems or controls documented within ninety calendar days of the change.</del>
<b>Response:</b> The suggested modification was not adopted. Where a requirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.					

**CIP-008-1 Incident Reporting and Response Planning**

**Summary Consideration:** There were no suggestions for modifications to the originally proposed VSLs for CIP-008-1 and none were made. The specific comments received are shown in the table below.

All Changes Proposed by Stakeholders for VSLs for CIP-008-1 Incident Reporting and Response Planning					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<i>Comment: OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!</i>			
<b>Response:</b> Thank you for your positive comment. Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.					
IRC SRC, IESO	R2	<i>Comment: OK</i>			
<b>Response:</b> Thank you for your positive comment.					

**CIP-009-1 Recovery Plans for Critical Cyber Assets**

**Summary Consideration:** There were some suggestions for modifications to the originally proposed VSLs for CIP-009-but none were adopted. The specific comments received are shown in the table below.

All Changes Proposed by Stakeholders for VSLs for CIP-009-1 Recovery Plans for Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R1	<i>Comment:</i> OK as the subrequirements' violations are "rolled-up" but each of the subrequirements has a VRF, which by FERC's rule has to have a VSL!			
<b>Response:</b> Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy.					
SoCal	R1	The Responsible Entity has documented but not annually reviewed recovery plan(s) for Critical Cyber Assets.	The Responsible Entity has created recovery plan(s) for Critical Cyber Assets but did not address one of the requirements CIP-009-1 R1.1 and R1.2.	The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-1 R1.1 and R1.2.	<del>The Responsible Entity has not created recovery plan(s) for Critical Cyber Assets that address at a minimum both requirements CIP-009-1 R1.1 and R1.2.</del>
<b>Response:</b> The suggested modification was not adopted. Where a requirement has performance that can be graded, there must, at a minimum, be a description of noncompliant performance that is Severe, indicating that most or all of the required performance was not met.					
IRC SRC, IESO	R2	<i>Comment:</i> Should be graded according to the delay in exercising the recovery plan.			
<b>Response:</b> The drafting team considers this to be a binary requirement.					
SoCal	R2			The Responsible Entity's recovery plan(s) have not been exercised at least annually.	<del>The Responsible Entity's recovery plan(s) have not been exercised at least annually.</del>
<b>Response:</b> The drafting team considers the requirement to be binary. Where a requirement or subrequirement is binary, it is not conducive to graded VSLs, and a failure to meet the required performance can only be categorized as a "Severe" VSL.					
IRC SRC, IESO	R3	<i>Comment:</i> OK			
<b>Response:</b> Thank you for your positive comment.					

All Changes Proposed by Stakeholders for VSLs for CIP-009-1 Recovery Plans for Critical Cyber Assets					
Company	R #	Alternate Lower VSL	Alternate Moderate VSL	Alternate High VSL	Alternate Severe VSL
IRC SRC, IESO	R4	<i>Comment: Should be graded according to the failure to meet the two conditions in R4: processes and procedures for the backup and storage of information required.</i>			
<b>Response:</b> Because some entities will not have separate processes and procedures, this suggestion was not adopted.					
IRC SRC, IESO	R5	<i>Comment: Should be graded according to the delay in completing the annual testing.</i>			
<b>Response:</b> The drafting team considers this requirement to be binary.					

2. If there any other comments you wish to provide (relative to the VSLs for CIP-002-1 through CIP-009-1) to the drafting team for Project 2008-14 Cyber Security Violation Severity Levels (version 1 VSLs) that you have not already provided in responses to the questions above, please provide them here.

Organization	Question 4 Comment
IESO IRC Standards Review Committee (IRC SRC, IESO)	<p>We did not fill out any of the tables above since we feel that it would more meaningful to offer the following high-level comments for the SDT's consideration as it revises the VSLs. Table 1, attached, provides a summary assessment of each of the VSLs proposed for the Version 1 CIP standards. Please also refer to Table 1 for the specific examples cited in the comments below.</p> <ol style="list-style-type: none"> <li>1. The existing standard structure and quality do not lend themselves to the development of appropriate and effective VSLs. There are still VRFs assigned to the subrequirements which according to FERC need to have VSLs. This makes it very convoluted to develop the main requirement's VSLs which to a good extent depend on the failure to comply with any of the subrequirements which may have multiple levels of VSL themselves. Further, a key problem arises when the main requirement is assign a binary VSL (Severe) while its subrequirements are graded. Often, the main requirement and some of its subrequirements are of similar nature. Hence, a violation of that similar natured requirement will subject an entity to double penalties.                       This is the problem we cited in the NERC's filing on the 322 VSL sets in the beginning of the year. The industry will need to continue to deal with this misfit issue until the requirements themselves are revamped and restructured.                       The remaining comments provided in the Comment Form are developed ignoring this issue, i.e., the way the standards are written not how they be written, and deal with the VSLs proposed for each main and subrequirement and look for consistency among the VSLs assigned to the requirements.</li> <li>2. Some VSLs can be graded, but they are treated as binary. Some examples are (not exhaustive): R1 and R1.2 in CIP-002-1, R2 and R4.2 in CIP-003-1, R2.3 and R3.2 in CIP-007-1. Suggestions to grade these requirements and other such requirements are provided in Table 1.</li> <li>3. Some requirements are assessed complete failure (Severe) if any one of the subrequirements is not met. This is clearly unacceptable since if the argument is that failing one of them essentially fails the bulk of the intent of the main requirement, then what about failing one of the remaining subrequirements? Do they all rise up to the level that failing any one would mean failing the bulk of the intent of the main requirements?                       Examples are: R4 in CIP-005-1, R8 in CIP-007. Detailed suggestions to make this change grade are provided in Table 1.</li> <li>4. Some subrequirements' violations are "rolled-up" to determine the main requirements' VSLs, which is the proper way. However, this approach is not consistently applied and in some cases where it is applied, there are no VSLs proposed for the subrequirements despite they are assigned VRFs. This is not consistent with the approach applied elsewhere in the CIP standards or the FERC directives. Examples are: R2, R3, R4 and R6 of CIP-006-1, R1 and R7 in CIP-007-1. A</li> </ol>

Organization	Question 4 Comment
	<p>consistent approach needs to be applied to all requirements.</p> <ol style="list-style-type: none"> <li>5. For requirements of similar nature, some are graded while others are not. This is inconsistent. Some examples re: R2.1 to R2.3 compared to R3.1 to R3.3 in CIP-003-1.</li> <li>6. Some requirements have listed under it, or included in the sentence, a number of conditions to be met yet the VSLs make no mention of these conditions. Examples are: R1 of CIP-004-1 and R1 of CIP-006-1.</li> </ol>
<p><b>Response:</b> Note that the drafting team took your comments on the individual VSLs and moved these so they appear in line with other comments related to the same set of VSLs.</p> <ol style="list-style-type: none"> <li>1. While the DT agrees that the existing standard structure makes it difficult to develop VSL (some better than others), the FERC directive must be met. The DT has addressed your concern (as well as that of man Please see the summary response to comments to see why the drafting team elected to develop a set of VSLs for each requirement and subrequirement to the extent it could do so without writing VSLs that lead to double jeopardy. In a few situations, the drafting team could not come up with a set of VSLs for the primary requirement that didn't duplicate what was in the subrequirements, and in those few instances, the drafting team did use the "roll up" methodology. With the roll up methodology, a single set of VSLs is developed to address the performance of the requirement in its entirety. While this approach has not been approved by FERC, it will be presented in a filing to FERC (as requested by FERC) showing all of the requirements where this approach would be used so that FERC can see a complete picture. Note that many of the requirements in the Version 1 Cyber Security standards contain subrequirements that could easily be stand-alone requirements. For these subrequirements, the use of the roll up method of developing VSLs would not be appropriate.</li> <li>2. In each situation where the IRC SRC, IESO recommended changing a binary requirement to a graded requirement, the drafting team either provided its reason for keeping the requirement as binary, or the drafting team changed the VSLs to represent a graded approach to identifying categories of noncompliant performance.</li> <li>3. In each situation where the IRC SRC, IESO recommended a specific change to a VSL, the drafting team either adopted the recommendation or provided its reason for not adopting the recommendation. For example, the VSLs for CIP-005-1 R4 were modified to use a percentage approach to categorizing noncompliant performance.</li> <li>4. The drafting team developed the initial set of VSLs before receiving information that FERC might accept the "roll up" method of developing VSLs. The team took a very conservative approach to using the roll up method as identified in response #1 above. If the drafting team had more time to refine the VSLs, the team would applied the "roll up" approach to more of the VSLs. Unfortunately, the drafting team has to complete its work, including the balloting of the VSLs, in time to file the VSLs with FERC by June 30. If FERC adopts the "roll up" method of VSLs, the Cyber Security VSLs can be modified and re-filed at a later time.</li> <li>5. The VSLs for CIP-003-1 R2.1 to R2.3 were modified so they closely align with the VSLs for R3.1 to R3.3.</li> <li>6. In CIP-004-1 R1, the bulleted items in the list are prefaced by the phrase, "such as" – and this means that these are suggestions, but are not required. The items listed under CIP-006-1 R1 all have individual sets of VSLs and if these items were also identified in the VSLs for the</li> </ol>	

**Consideration of Comments for Project 2008-14 — Cyber Security Version 1 Violation Severity Levels**

Organization	Question 4 Comment
<p><b>primary requirement, responsible entities would have concerns about double jeopardy.</b></p>	
<p>NPCC</p>	<p>In the CIP-004-1 R1 version 1 VSL the “(implemented)”/“(implement)” should be removed because it is not in the Standard. Remove “(for example, dial-up modems) from CIP-005-1 R1.1 because examples can be misleading. Several requirements specify percentage thresholds in their VSLs. What is the basis for those thresholds? In CIP-005-1 R4, the VSL identifies what has been demonstrated in accordance with the Standard. This is inconsistent with other VSLs that identify what has not been demonstrated. Because of this, the percentage threshold numbers are not consistent.</p>
<p><b>Response: The drafting team did remove the various versions of the word, “implement” from the VSLs for CIP-004-1 Requirement R1. The parenthetical phrase that appeared in the VSL for CIP-005-1 R1.1 was used in the requirement. The percentages are based on support of the criteria for setting VSLs and from FERC guidance in the VSL Order. In general, the thresholds for the various VSLs are missing up to 5% is Lower; missing from 5-10% is Moderate; missing 10-15% is High and missing more than 15% is Severe. Other percentages are acceptable as long as they are defensible. The team revised the VSLs for CIP-005-1 R4 so they describe the “noncompliant” performance rather than the compliant performance.</b></p>	
<p>Kansas City Power &amp; Light</p>	<p>If an entity is performing the requested action, lack of documentation should not be sufficient for a VSL greater than moderate. CIP-003 R6 VSL appears to require 2 processes one for configuration management and one for change control, whereas the standard can be interpreted to require only one.</p>
<p><b>Response: Where documentation is used as evidence that a requirement has been accomplished, there is no way of proving that the entity is compliant if there is no documentation. Violation Risk Factors (VRFs) assess the reliability-related risk to the bulk electric system of the violation of a requirement – Violation Severity Levels do not assess the reliability-related risk – VSLs categorize degrees of noncompliant performance. In other words, the VRF says what is the possible impact to the BES if you violate a requirement – and the VSL is used to describe how badly the performance was missed. Agree that CIP-003-1 Requirement R6 can be interpreted as requiring either one or two processes – the proposed VSLs work for either interpretation since a single process that addresses both change control and configuration management would meet the requirement as well as two separate processes.</b></p>	
<p>Tampa Electric</p>	<p>See general comments, we really need the VSLs to focus on measuring the effectiveness of the program rather than the existence or accuracy of documentation.</p>
<p><b>Response: The drafting team addressed the general comments within the comments related to specific suggestions for modifications to VSLs.</b></p>	
<p>AEP</p>	<p>It appears that the severity levels, as drafted, start from the severe level and follow a graduated scale down to the lower VSL. It</p>

Organization	Question 4 Comment
	<p>appears that this is an arbitrary assignment, especially for binary VSLs. We would suggest that, if selected by a default starting position, the VSLs should be centered on the moderate level and expand in either direction as appropriate.</p>
<p><b>Response: VSLs categorize degrees of noncompliance, with up to four categories for each requirement – but for each requirement it is possible to be found “fully noncompliant” (the criteria for Severe VSL) it is not always possible to define noncompliance that is “mostly compliant” – the criteria for a Lower VSL. Thus there will always be more “Severe” VSLs than “Lower” VSLs in the total population of VSLs.</b></p>	
<p>Southern California Edison Company</p>	<ol style="list-style-type: none"> <li>1. The VSLs drafted for CIP-002-1 through CIP-009-1 double-count violations for Requirements and Sub-Requirements, for example, a violation to CIP-003-1 R2 will inherit violations to R2.1, R2.2 or R2.3.</li> <li>2. CIP-007 R2.2 and R2.1 are redundant, and represent the same violation.</li> <li>3. When viewed as a whole, the ratings are inconsistent from one requirement to the next and do not appear to consider the criticality of the item in question. For instance, failure to annually review recovery plans for CCAs is rated as Moderate, while failure to document changes to the senior manager’s phone number within 30 days is rated as Severe. Variations in like-measurements occur throughout. For instance, missing elements for one document will be rated as Moderate, another as Severe, and yet another with a full spectrum based on the percentage of completion. In most cases, the type of document is similar with no significant variance in risk.</li> </ol>
<p><b>Response: The drafting team tried to identify VSLs for main requirements that did not measure the same noncompliant performance as identified for any associated subrequirements.</b></p> <p><b>The drafting team is not in a position to make any modifications to the requirements.</b></p> <p><b>The drafting team tried to be as consistent as possible in setting VSLs. In some requirements, missing a single item may result in the process or product mostly missing the reliability-related objective of the requirement. In this case, the VSL for missing a single element may be “Severe.” In another case missing a single element of a process may have only a marginal impact on the process and may be “Lower.” Note that when a requirement is “binary” or “pass/fail” then noncompliance will always be “Severe.”</b></p>	

3. The drafting team assigned to develop the V1 VSLs has proposed expanding the scope of its SAR to also include development of VSLs for the Cyber 706 SDT. Do you agree with the proposed expansion in the scope of the SAR for V1 Cyber Security VSLs?

**Summary Consideration:** Most commenters who responded to this question indicated support for the expanded scope of the SAR.

Organization	Yes or No	Question 5 Comment
Tampa Electric	Disagree	We believe that these VSLs as currently defined do not truly look at the effectiveness of controls. We believe that the CSDT is in the best position to evaluate the measures for effectiveness of cyber security controls and should perform this function.
<p><b>Response:</b> VSLs are intended to categorize degrees of noncompliant performance. Violation Risk Factors (VRFs) assess the impact a violation of a requirement can have on the bulk electric system. VSLs and VRFs are not the same.</p>		
Southern California Edison Company	Agree	
Exelon	Agree	
IESO	Agree	
MRO NERC Standards Review Subcommittee	Agree	
Kansas City Power & Light	Agree	
AEP	Agree	
IRC Standards Review Committee	Agree	