Project 2008-06 - Cyber Security Order No. 706 - V5

Working Draft (September 11, 2012) of Consolidated VSLs from all standards

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES	Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and	Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and	OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium	medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;	BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible	at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			BES Cyber Systems have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous approval. (R2)	calendar months of the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices and associated physical security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices and associated physical security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to	OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a	The Responsible Entity has a program for	The Responsible Entity has a program for	The Responsible Entity did not have all of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and	required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,	not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel	physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and	checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized	did not identify, assess, and correct the deficiencies. (3.5)	did not identify, assess, and correct the deficiencies. (3.5)	for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System	storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's	Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR	access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9)	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct deficiencies. (1.9)	(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for unauthorized access through a physical access point into a Physical security Perimeter or to communicate such

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry through any Physical Security Perimeter with sufficient information to identify the individual and date of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day Operations**	**Medium**	N/A	The Responsible Entity included a visitor	The Responsible Entity included a visitor	The Responsible Entity has failed to include or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				control program that requires logging of each of the initial entry and last exit dates and times of the visitor on a daily basis, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the	control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has documented and implemented a maintenance and	The Responsible Entity has not documented and implemented a maintenance and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			testing program for Physical Access Control Systems, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	testing program for Physical Access Control Systems, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	testing program for Physical Access Control Systems, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	testing program for Physical Access Control Systems. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but did not complete required testing within 27 calendar months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65	document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did	calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or	OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated	deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		correct the deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of identified malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and	did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security	The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems	applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	(per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did	(per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not	of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not	not assess or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented	more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, or correct the deficiencies. (5.6)	identify, assess, or correct the deficiencies. (5.6)	process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	(2.1) The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident.	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident	(3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response groups or individuals, or • Technology changes.		

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected(2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Technology changes.	• Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any disposal or reuse processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset as specified in R 2. (2.1)