NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Assessing and Reducing Risk Reference Document

Security Working Group

Introduction

NERC's Reliability and Security Technical Committee (RSTC) develops reference documents as a resource for the electric utility industry and/or NERC stakeholders regarding a specific topic of interest through its subcommittees and working groups. These documents are intended to reflect industry practices or technical concepts at the time of publication and may be updated upon recommendation by the RSTC or its subgroups to reflect current industry practices if necessary as described in the RSTC Charter.[1]

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reference documents are not binding norms or parameters; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices described in this reference document. Entities should review this document in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed; these changes should be done with consideration of system design, configuration, and business practices.

Executive Summary

This reference document is comprised of instructions and a risk assessment tool that can help organizations determine their current security and compliance posture. The tool is a Microsoft Excel-based spreadsheet that maps requirements of the CIP Reliability Standards to the National Institute of Standards and Technology (NIST) Cybersecurity Framework[2] (hereafter referred to as "the framework"). It can help a responsible entity identify gaps in their current environment and develop an improvement plan for addressing them.

The instructions and tool were the result of a collaborative effort by industry volunteers from the RSTC, Security Working Group (SWG), and representatives from NERC and NIST. The deliverables associated with the reference document underwent a pilot study with SWG members; their recommendations were incorporated into the final version.

Background

NIST's mission is to promote United States innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. As a part of its mission, NIST has developed standards, special publications, and guidelines on various topics, including cybersecurity. In February 2014, NIST published the original Cybersecurity

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_approved20191105.pdf
[2] https://www.nist.gov/cyberframework

Framework based on existing standards, guidelines, and practices for reducing cybersecurity risks. The Framework provides a prioritized, flexible, repeatable, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties.

In January 2020, NERC and NIST representatives approached the SWG to review the Framework Version 1.1 mapping[3] and update it to align with the current version of the CIP Reliability Standards.

The SWG team that produced this reference document had the following objectives:

- **Vision**
  - Provide responsible entity subject matter experts or practitioners with the capability to assess current compliance and security posture and develop a roadmap and/or business justification to reach risk levels per their organization's acceptable risk appetite.
- **Deliverables**
  - **Documentation:** A reference document that describes a methodology for performing a self-assessment, directions for using the self-assessment tool, potential use cases for identifying gaps in compliance or programs, and assistance in developing risk basked business justifications for improvement
  - **Tool:** Spreadsheet to self-assess compliance with CIP requirements and security practices and prioritize risk management strategies based on the self-assessment results

Methodology

This reference document highlights the relationships between the CIP Reliability Standards' requirements and cybersecurity outcomes. "Outcomes" provides a common language for assessing, understanding, and communicating the results for managing cybersecurity-related risk to internal and external stakeholders without limiting the focus to compliance.

The methodology used to develop this reference document leverages the external sources that are listed below:

- **Authoritative Documents**[4]
  - **NERC CIP Reliability Standards:** The cybersecurity requirements for reliable operation of the North American BPS
  - **NIST Cybersecurity Framework V1.1:** A set of activities to achieve specific cybersecurity outcomes and informative reference examples of guidance how to achieve them
- **Informative References**

[3] Mapping of CIP Standards to NIST Cybersecurity Framework (CSF) v1.1

[4] Note: mechanisms and processes being implemented to update the self-assessment tool to reflect authoritative document changes

  - Standards, guidelines, and practices that illustrate a method to achieve the cybersecurity outcomes, as cited in the framework

- **Relationships:** The association of framework outcomes to CIP requirements to inform overall cybersecurity posture, program, and risk management practice maturity:
  - **Compliance:** Outcomes that directly relate to and support compliance and cybersecurity requirements
  - **Cybersecurity:** Although not directly applicable to compliance with the CIP Reliability Standards, associated framework outcomes provide cybersecurity program assurance

Self-Assessment Tool Usage Instructions

"**Appendix: Self-Assessment Tool Design and Logic**" contains explanations of the design and logic of the tool, including screen shots. These instructions describe how to use the self-assessment tool:

1. **Required:** Read the "Instructions" tab of the self-assessment tool that mirror these instructions.
2. **Optional:** Familiarize yourself with the "Implementation Tier" short descriptions on the data_validation_values tab of the self-assessment. You may wish to print those and have them on hand when performing the self-assessment.
   a. Implementation tiers are a direct copy of the tiers as described in the NIST framework.
   b. Implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage risk.
   c. The tool provides the capabilities for changing the implementation tier short descriptors to suit your organizations terms if so desired in cells B2:B5.
3. **Optional:** If not intimately familiar with the CIP requirements, review the "CIP Standards" tab and/or the link included in the instructions to NERC's CIP Reliability Standards for the detailed requirements associated with each CIP Reliability Standard.
4. **Optional:** For a list of security standards, guidelines, and practices that map to each framework sub-category, see the "Cyber Security Framework" tab. The associated standards can be used to analyze your organization's internal controls or cybersecurity program to identify potential gaps.
5. **Required:** On the "Self-Assessment" tab, perform a risk self-assessment of your organization's CIP standards compliance and cybersecurity practices by selecting from Column I the tier that best represents your implementation level/status of associated outcome.

   Note: the self-assessment tool is intended for CIP requirement owners or practitioners responsible for the creation and implementation of the security controls
6. **Optional:** The tool includes the capability to modify the provided relationships for each framework sub-category to the associated CIP requirements if so desired. The process for modifying relationships is described below:
   a. Select an alternate relationship from the available drop-down list of Column H.
   b. If different and/or a set of alternative relationships are desired, provisions have been built into the tool to do so on the "data_validation_values" tab in cells B16:B20.
7. **Required:** Review the self-assessment results on the "Implementation Dashboard" tab. This tab is automatically updated based on the information entered on the "Self-Assessment" tab. Results displayed are as follows:
   a. Column E (Average Implementation Score) shows the average implementation of the associated framework sub-categories. Conditional color formatting is used to show levels of risk based on the level of implemented cybersecurity-related risk management practices (larger numbers = higher implementation levels with lower risk):

Green for > 3.5 (low risk)

Yellow for 2.5 to 3.5 (minimal risk)

Orange for 1.5 to 2.5 (moderate risk)

Red for 1.0 to 1.5 (high risk)

b. Column H (CSF-ID to CIP relationship) identifies compliance or cybersecurity-related categories related to an associated CIP requirement that could be used to prioritize risk treatment activities based on the risk focus of your organization.

c. Column I (Cybersecurity Risk Management Tier) represents the implementation tier of the framework sub-category outcomes associated with a given CIP requirement.

   i. Level 1 represents low or immature capabilities and Level 5 represents high or very mature capabilities.

Note: Column J contains the descriptor with the associated Implementation Tier from the "data validation values" tab in cells B2:B5.

Self-Assessment Results Use Cases

The following are potential suggested use cases of the self-assessment results on the "Implementation Dashboard" of the self-assessment tool:

1. **CIP Violation Risk Factor focus:** filter on Column D (VRF) to identify VRF with a low average implementation scores in Column E to identify potential CIP Violation Risk Factor compliance improvement opportunities
2. **CIP Compliance focus:** filter on Column H (CSF-IT to CIP Relationship) for "compliance related" relationships (or your equivalent alternative you may have added) to identify potential CIP compliance improvement opportunities based on associated risk implementation tier noted in columns I and J
3. **Cybersecurity focus:** filter on Column H (CSF-IT to CIP Relationship) for "cybersecurity related" relationships (or your equivalent alternative you may have added) to identify potential cybersecurity compliance improvement opportunities based on associated risk implementation tier noted in columns I and J

Regardless of focus, results can be used to develop business justification for annual budget and resource planning purposes that are focused on security and compliance risk reduction. Results can also be used to develop a long-term improvement roadmap.

In all cases, responsible entities are encouraged to leverage the informative references of the Framework; they can be used in the following manners:

- **Center for Internet Security (CIS) Top 20 Critical Security Controls:**[5] Technology teams leverage the CIS top 20 security controls to review IT internal controls.
- **Security Programs:** Cybersecurity teams utilize NIST 800-53 or ISO27001 comprehensive security controls to compare implemented security programs.
- **Governance:** Governance and oversight teams utilize COBIT security controls to review IT governance and management practices.
- **Industrial Control/OT:** Control system operations leverage the ISA 62443 security controls to review implemented security protection measures.

SWG Task Force Members

The following is the list of SWG task force members who volunteered to develop this reference document, associated self-assessment tool and overview PowerPoint.

Keith St. Amand (project lead)
Midcontinent Independent System Operator

Dan Wagner / Aldo Nevárez
Western Electricity Coordinating Council

Monica Jain
Southern California Edison

Brenda Davis
CPS Energy

Mike Johnson
Pacific Gas & Electric

Karl Perman
Department of Water Resources California

Jeff Marron
National Institute of Standards and Technology

Matthew Light
Western Area Power Administration

[5] https://www.cisecurity.org/controls/cis-controls-list/

Appendix: Self-Assessment Tool Design and Logic

The self-assessment tool described by this reference document is based on Microsoft Excel (see **Figure 1**) and provides a mechanism for the owners of CIP standards and requirements to perform a simple rating of their current risk implementation levels and obtain a "dashboard" with actionable criteria to focus on and communicate to stakeholders.

Note: this self-assessment tool was tested by a volunteer set of SWG member companies; their feedback and update suggestions were incorporated into this reference document and the self-assessment tool.

Figure 1: Excel Workbook Tabs

Tabs: The Excel workbook includes the following tabs and associated descriptions:

- **Instructions:** contains intended use, background, benefits, tab descriptions, and self-assessment usage instructions
- **Implementation Dashboard:** presents the results of the Self-Assessment tab; results depicting summary score of each the framework sub-category associated with a CIP requirement
- **Self-Assessment:** maps CIP requirements aligned to the Framework categories (Objectives) and sub-categories (outcomes) with a cybersecurity risk management tier selection item for CIP requirement owner to choose
- **CIP Standards:** contains unique IDs, purpose + requirements, and violation risk factor (VRF) ratings associated with each requirement (Columns B and C are direct copies from the standards (Column A is provided to facilitate Excel pivot table and formula functionality.)

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize future maintenance and update efforts of the tool.
- **Cyber Security Framework**: contains information downloadable and available directly from the NIST Cybersecurity Framework

  Note: this tab is for reference purposes only and is used in the first two tabs to minimize maintenance and update efforts.
- **Pivot Tables:** contains Excel pivot tables that depict the cross-references of CIP requirement ID to the Framework Sub-Category ID and the Framework Sub-Category to CIP to CIP requirement IT

  Note: The purpose of these cross-references is to facilitate independent analysis if needed/desired.
- **data_validation_values:** Lists the Excel "named references" used throughout the workbook They include the following features:

- The capability of changing the implementation tier descriptions if the native framework risk implementation tiers are not preferred
- A description for the framework risk tiers
- A description of the CIP to the framework relationships used in the tool

Note: The SWG team designed the tool to minimize the effort needed to update and maintain the tool. Plans are to update the tool as required to reflect changes to the CIP requirements or to framework updates are released.

To permit maximum flexibility by users, none of the tool's cells or tabs are password protected. Users should be aware that some changes could have unintended results on other tabs and cells that affect the results.

- **Implementation Dashboard Tab (see Figure 2)** contains cell formulas in all but Column A and F to automatically update cell contents
  - Column C and D contents updated based on matching row in the CIP Standards tab
  - Column E is the average calculated from the corresponding Risk Management Tier values in Column I
  - Column G contents updated based on matching row in the Cyber Security Framework tab
  - Column H was filled in based on the analysis for the SWG task force team and feedback from testing volunteers
  - Column J contents based on the corresponding value from the data validation values tab
  - Color Conditional formatting:
    - Column D: red for high, brown for medium, green for lower
    - Column E: green for > 3.5, yellow for 2.5–3.5, orange for 1.5–2.5, red for 1.0–1.5 (in order to avoid applying color formatting to blank rows)
    - Column J: dynamic formula based on the matching tier on the data validation values tab

A	C	D	E	F	G	H	I	J
CIP Requirement	**CIP Standard Purpose and Requirement**	**VRF Rank**	**Average Impl Score**	**CSF-ID**	**NIST CSF Sub-Category Description *Outcomes***	**Sub-Catergory CIP Relationship**	**Cyber Security Risk Mgmt Tier**	**Risk Tier Descriptor**
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 2: Implementation Dashboard Tab

- **Self-Assessment Tab (see Figure 3)**
  - All cell contents are populated based on formula reading from either the CIP standards, cyber security framework, or data validation values tabs—the intent is to simplify future maintenance update efforts.

A	B	C	D	E	F	G	H	I
	CIP	**NIST CSF**	**CSF ID**	**NIST-CSF Category**	**NIST CSF ID**	**NIST-CSF Sub-Category**	**Cybersecurity**	**Risk Tier**
CIPv5 ID	**Requirement and Parts**	***Function***	***Cat***	***Objectives***	***Sub-cat***	***Outcomes***	***Risk Mgmt Tier***	***Descriptor***
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 3: Self-Assessment Tab

- **CIP Standards Tab (see Figure 4):** A compilation of the current effective CIP standards subject to enforcement as posted on the NERC CIP Standards[6] site

  Note: normalized/standardize ID in Column A were created in order to facilitate linkage between the various tabs, filtering, and pivot table capabilities

[6] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

A	B	C
CIP ID	Purpose and Requirements	VRF Rating
CIP-002-5.1a-R1	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 1:** Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH
CIP-002-5.1a-R2	**Purpose:** To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. **Requirement 2:** The Responsible Entity shall: ***(See Sub-Requirements 2.1 and 2.2)***	LOWER

Figure 4: CIP Standards Tab

- **Cyber Security Framework Tab (see Figure 5):** contains a modified download of the Excel file available from the framework site.[7] The only modification was to place the informative references into individual columns as opposed to including them all in a single cell for each sub-category.

  Note: normalized/standardized IDs were created in order to facilitate linkage between the various tabs, filtering, and Pivot Table capabilities

A	B	C	D	E	F	G	H	I	J
		Outcomes		*Outcomes*	*Informative References*				
Function		Category	ID	Sub-Categories	*NIST 800-53 Rev*	*CIS CSC*	*COBIT*	*ISA*	*ISO*
	ID.AM	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-01**	Physical devices and systems within the organization are inventoried	CM-8, PM-5	CIS CSC 1	BAI09.01, BAI09.02	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
			ID.AM-02	Software platforms and applications within the organization are inventoried	CM-8, PM-5	CIS CSC 2	BAI09.01, BAI09.02, BAI09.05	ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8	ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1
			ID.AM-03	Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8	CIS CSC 12	DSS05.02	ISA 62443-2-1:2009 4.2.3.4	ISO/IEC 27001:2013 A.13.2.1
			ID.AM-04	External information systems are catalogued	AC-20, SA-9	CIS CSC 12	APO02.02, APO10.04, DSS01.02	N/A	ISO/IEC 27001:2013 A.11.2.6
			ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6	CIS CSC 13, 14	APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02	ISA 62443-2-1:2009 4.2.3.6	ISO/IEC 27001:2013 A.8.2.1
			ID.AM-06	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11	CIS CSC 17, 19	APO01.02, APO07.06, APO13.01, DSS06.03	ISA 62443-2-1:2009 4.3.2.3.3	ISO/IEC 27001:2013 A.6.1.1

Figure 5: Cyber Security Framework Tab

- **Data validation Values (see Figure 6):** primarily for lookup and Excel "named references" purposes used throughout the workbook:

[7] https://www.nist.gov/cyberframework/framework

- **Customization:** cells B2–B5 are unlocked, if a responsible entity does not like the Risk Implementation Tiers as provided by the framework. Changing those to whatever an entity prefers, will automatically update the correspond values on the other sheets.

Note: Cells C2–C5 are for reference purposes only, describing the conditional formatting colors used on the Implementation Dashboard corresponding to the associated Implementation Tier #.

	A	B	C
1	Implementation Tier	Description	Condiitonal formatting applied
2	1	Partial	Red
3	2	Risk Informed	Orange
4	3	Repeatable	Yellow
5	4	Adaptive	Green
6			

Figure 6: Data Validation Values Tab: Customization #1

- **Customization (see Figure 7)**: Cells A16 and A17 are unlocked if a responsible entity wishes to use different text to describe.

	A	B
15	Relationships	Descriptions
16	directly Relates	*There are clear and/or direct relationships between the CSF Sub-Category and CIP Requirement*
17	indirectly Relates	*NIST-CSF Focal Document element is a subset of the CIP Reference Document element*

Figure 7: Data Validation Values Tab: Customization #2

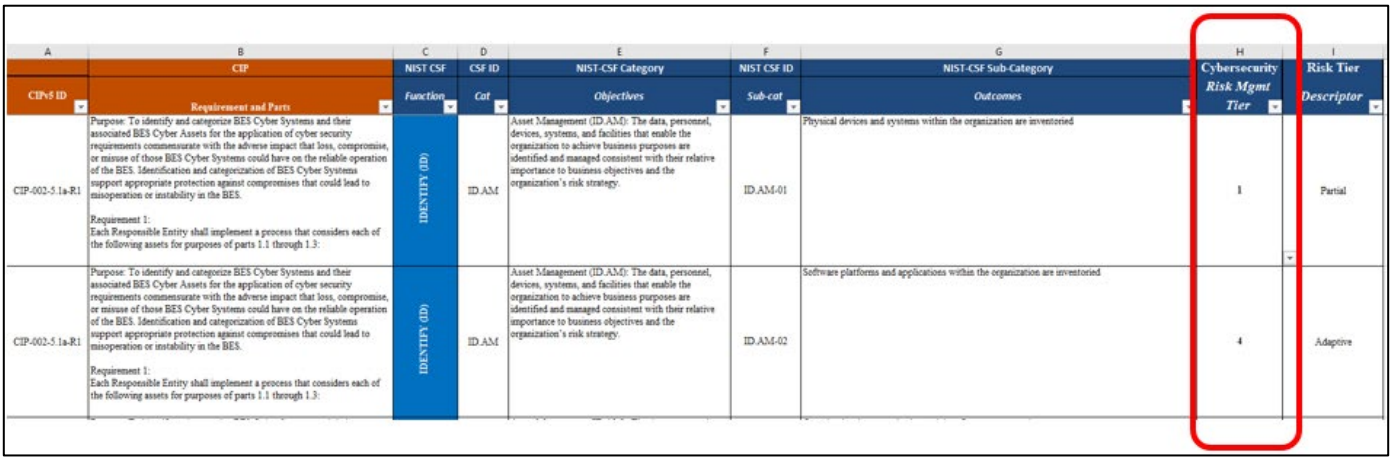
Design Assumptions

- Each responsible entity will have implemented their own security controls that are often based on the same security guidance identified in the framework informative references.
- Generally, there are separate CIP requirements owners assigned within responsible entity companies and usually develop associated policies, controls, and/or practices.
- By providing a cross-mapping of the CIP standards to the framework sub-categories, requirement owners can view the associated informative reference practices to compare their implemented security controls against.
- The Implementation Dashboard tab summary results will help identify gaps and/or improvement opportunities.

Self-Assessment Tab Instructions (see **Figure 8**)

1. Either distribute the self-assessment tool spreadsheet to individual CIP requirement owners or gather all CIP requirement owners together to collectively review and assess their associated requirement implementation level.

2. CIP requirement owners review each of their associated CIP requirements and select the risk implementation level from the available drop-down number in Column H (Cybersecurity Risk Management Tier) that best represents their current practice implementation level.
3. Once completed, move on to review summary results in the Implementation Dashboard tab.



A	B	C	D	E	F	G	H	I
CIP		NIST CSF	CSF ID	NIST-CSF Category	NIST CSF ID	NIST-CSF Sub-Category	Cybersecurity	Risk Tier
CIPv5 ID	Requirement and Parts	Function	Cat	Objectives	Sub-cat	Outcomes	Risk Mgmt Tier	Descriptor
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-01	Physical devices and systems within the organization are inventoried	1	Partial
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	IDENTIFY (ID)	ID.AM	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-02	Software platforms and applications within the organization are inventoried	4	Adaptive

Figure 8: Completing Self-Assessment Tab

Implementation Dashboard potential Use Cases:

After all rows in the Self-Assessment tab (see **Figure 9**) have been completed, the implementation dashboard will represent the summary risk results by CIP requirement to highlight the following:

- Identify where there may be **CIP Violation** risks based on the VRF rank value in Column D and the corresponding average imply score in Column E
- Identify where there may be **Compliance** risks, based on the "Directly Relates" relationship in Column H and a corresponding low implementation level in Column J
- Identify where there may be **Security** risks, based on the "Indirectly Relates" relationship in Column H and a corresponding low implementation level in Column J

A	C	D	E	F	G	H	I	J
CIP Requirement	**CIP Standard Purpose and Requirement**	**VRF Rank**	Average Impl Score	**CSF-ID**	**NIST CSF Sub-Category Description** ***Outcomes***	**Sub-Catergory CIP Relationship**	**Cyber Security Risk Mgmt Tier**	**Risk Tier Descriptor**
CIP-002-5.1a-R1	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 1: Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:	HIGH	2.3	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	4	Adaptive
				ID.AM-03	Organizational communication and data flows are mapped	indirectly relates	4	Adaptive
				ID.AM-04	External information systems are catalogued	indirectly relates	3	Repeatable
				ID.AM-05	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	directly relates	2	Risk Informed
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial
CIP-002-5.1a-R2	Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. Requirement 2: The Responsible Entity shall: (See Sub-Requirements 2.1 and 2.2)	LOWER	1.0	ID.AM-01	Physical devices and systems within the organization are inventoried	directly relates	1	Partial
				ID.AM-02	Software platforms and applications within the organization are inventoried	directly relates	1	Partial
				ID.AM-04	External information systems are catalogued	indirectly relates	1	Partial
				ID.BE-04	Dependencies and critical functions for delivery of critical services are established	directly Relates	1	Partial
				ID.RA-04	Potential business impacts and likelihoods are identified	indirectly relates	1	Partial

Figure 9: Review Self-Assessment Results

References

- NIST Cybersecurity Framework 1.1: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NERC CIP Enforceable Standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- Mapping of NIST Cybersecurity Framework to NERC CIP v3/v5 November 2014 - https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/CSSWG-Mapping_of_NIST_Cybersecurity_Framework_to_NERC_CIP.pdf
- Mapping of CIP Standards to NIST Cybersecurity Framework v1.1 Updated: https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx (under Compliance | NIST)

Version History

SWG Reference Document Version History					
Version No.	**Date**	**Chapter**	**Page**	**Description**	**Version**
1	October 2020	All	All	Original Document	.1
2	November 12, 2020	All	All	Publications and Admin review complete	.2
3	June 8, 2021	All	All	Approved by RSTC, with direction to re-designate as a reference document rather than guideline	1
4	July 1, 2021	All	All	Edits to reflect the document's status as a reference document	1.1