الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Operational Technology Cybersecurity

Controls Methodology and Mapping Annex

(OTCCMM -1: 2022)

Sharing Notice: White
Document Classification: Public

Disclaimer: The following methodology will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients either inside or outside the organization, beyond the scope specified for receipt.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

Table of Contents

Table of Table

Table of Figures

Design Principles of the Operational Technology Cybersecurity Controls (OTCC)

The Operational Technology Cybersecurity Controls (OTCC) has been developed to provide more specific controls for OT/ICS systems. The OTCC document is an extension to the ECC-1:2018 cybersecurity controls. Thus, applicable organizations must comply with ECC controls first, and then comply with the additional controls provided by the OTCC-1:2022 document.

The following principles were taken into account while developing the OTCC document :

- The security requirements stated in the OTCC document are an extension to the security requirements in the ECC controls.
- The OTCC cybersecurity controls leverage existing work that has been practiced by other leading countries or international standards in OT/ICS fields.
- The OTCC cybersecurity controls were mapped to international documents in order to allow organizations to make use of international practices.

Relationship to International Standards

The following international standards, regulations, and guidelines related to OT/ICS environments were utilized as the foundation when developing the OTCC document:

- ISA/IEC 62443 Series on Security for industrial automation and control systems (IACS), specifically:
  - 62443-2-1, Draft 3, Edit 8 Committee Draft for Vote (Approved), Security program requirements for IACS asset owners.
  - 62443-3-2:2020, Security risk assessment for system design.
  - 62443-3-3:2013, System security requirements and security levels.

- US National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, also called the NIST Cybersecurity Framework (CSF).
- US NIST Special Publication (SP) 800-53 rev4, Security and Privacy Controls for

Federal Information Systems and Organizations.

- US NIST SP 800-82 rev 2, Guide to Industrial Control System (ICS) Security.
- 104 - Norwegian Oil and Gas Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems (NOG 104).
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 6.
- US Department of Energy (DoE) Cybersecurity Capability Maturity Model (C2M2).

Design Methodology of Operational Technology Cybersecurity Controls (OTCC-1:2022)

Relationship to Essential Cybersecurity Controls (ECC-1:2018)

Operational Technology Cybersecurity Controls (OTCC-1:2022) is an extension of Essential Cybersecurity Controls (ECC-1:2018). Figure 1 below shows that OTCC implementation starts after ECC implementation and compliance.

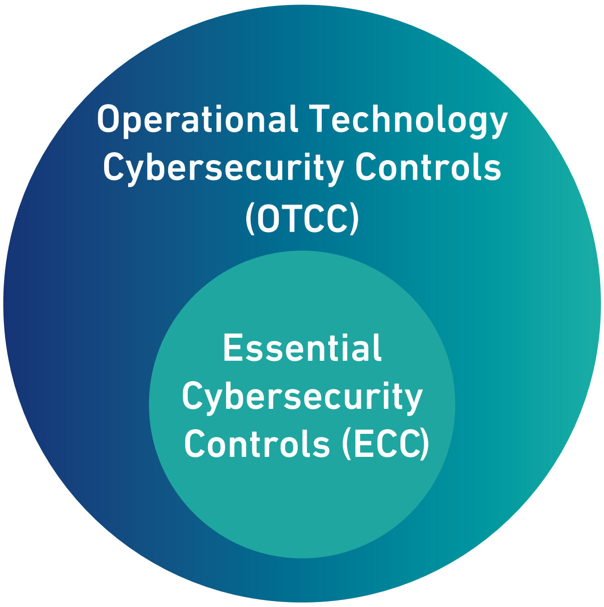
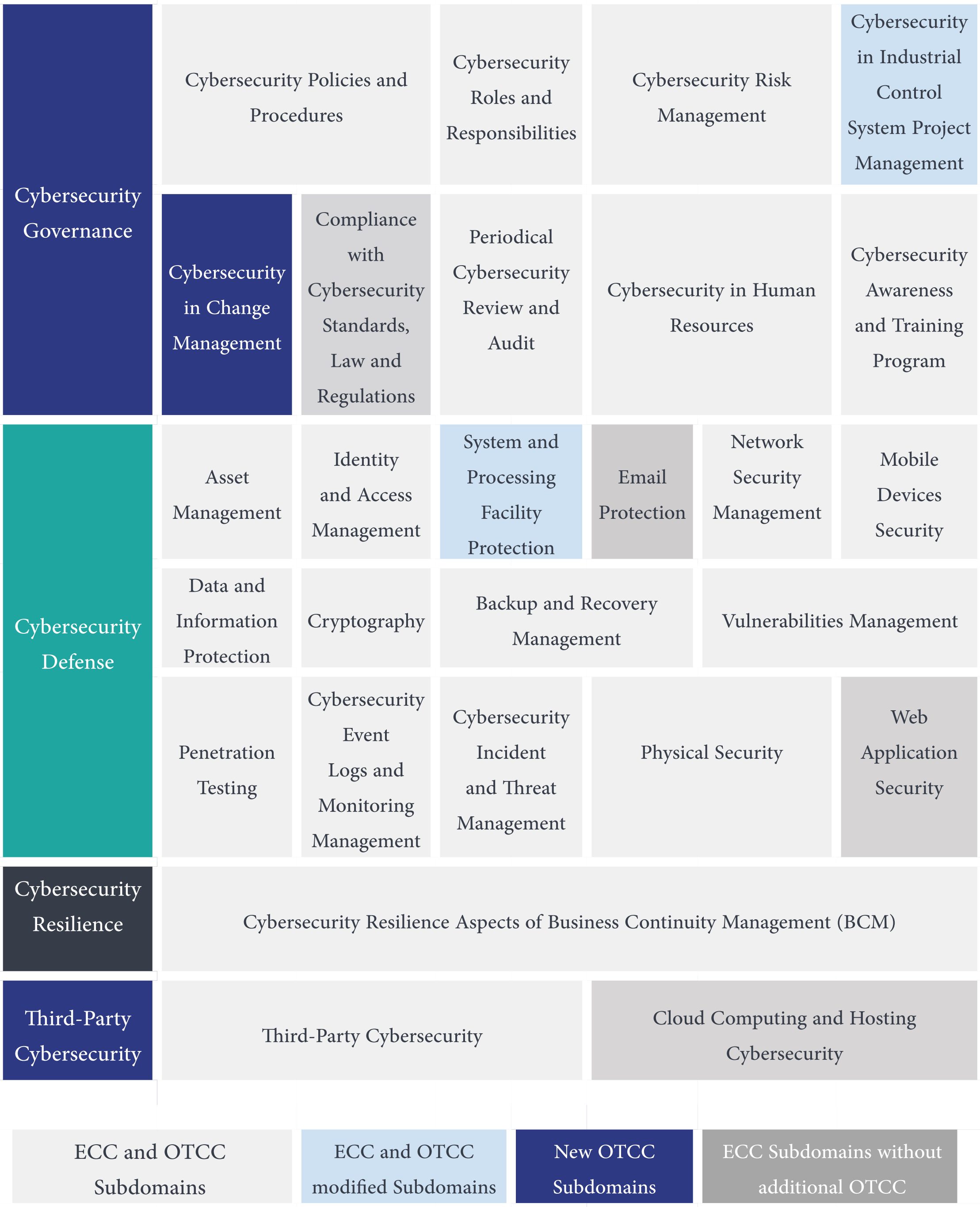

Operational Technology Cybersecurity Controls (OTCC)
Essential Cybersecurity Controls (ECC)

Figure 1: Overlapping Scope of OTCC and ECC

The main domains and subdomains of ECC and OTCC are aligned in a similar structure. Four of the five ECC main domains are in the OTCC. In addition, 20 subdomains of the ECC subdomains are OTCC subdomains with additional OT specific contorols. (shown in light grey in Figure 2). One new subdomain was added to the OTCC document (shown in dark blue in Figure 2). Two subdomains were modified in the OTCC document (shown in light blue in Figure 2). Four ECC subdomains do not have specific controls for OT/ICS environments (shown in grey in Figure 2).



Cybersecurity Governance

Cybersecurity Policies and Procedures

Cybersecurity Roles and Responsibilities

Cybersecurity Risk Management

Cybersecurity in Industrial Control System Project Management

Cybersecurity in Change Management

Compliance with Cybersecurity Standards, Law and Regulations

Periodical Cybersecurity Review and Audit

Cybersecurity in Human Resources

Cybersecurity Awareness and Training Program

Cybersecurity Defense

Asset Management

Identity and Access Management

System and Processing Facility Protection

Email Protection

Network Security Management

Mobile Devices Security

Data and Information Protection

Cryptography

Backup and Recovery Management

Vulnerabilities Management

Penetration Testing

Cybersecurity Event Logs and Monitoring Management

Cybersecurity Incident and Threat Management

Physical Security

Web Application Security

Cybersecurity Resilience

Cybersecurity Resilience Aspects of Business Continuity Management (BCM)

Third-Party Cybersecurity

Third-Party Cybersecurity

Cloud Computing and Hosting Cybersecurity

ECC and OTCC Subdomains

ECC and OTCC modified Subdomains

New OTCC Subdomains

ECC Subdomains without additional OTCC

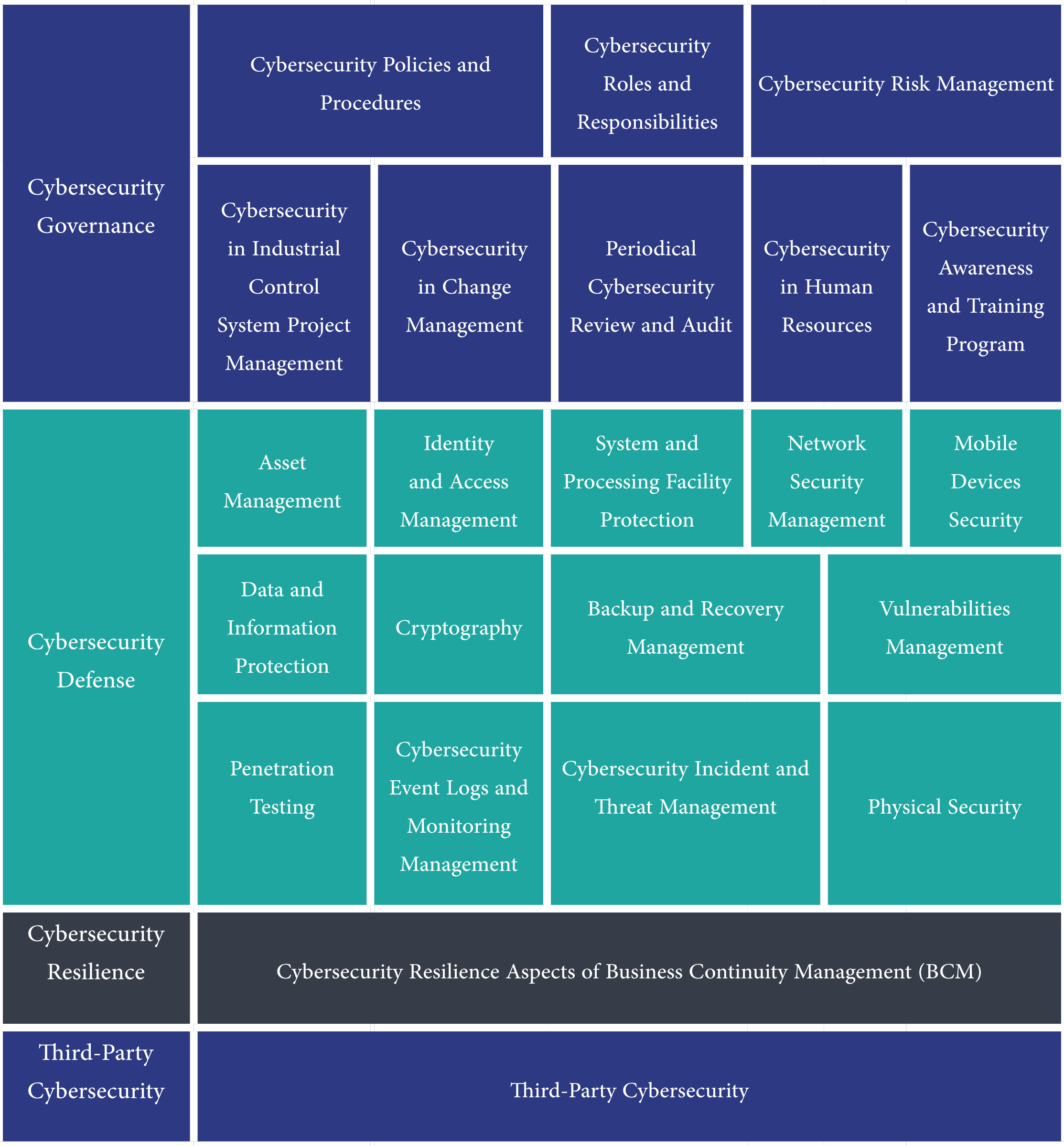
Figure 2: Relationship between OTCC and ECC Main Domains and Subdomains

Relationship to Critical Systems Cybersecurity Controls (CSCC-1:2019)

Operational Technology Cybersecurity Controls (OTCC-1:2022) is applicable to industrial control systems or operational technologies residing in critical facilities. Non-OT/ICS critical systems are subject to Critical Systems Cybersecurity Controls (CSCC-1:2019) while critical industrial control systems and operational technologies are only subject to Operational Technology Cybersecurity Controls (OTCC-1:2022).

Main Domains and Subdomains Structure of the OTCC

Figure 3 shows the structure of OTCC Main Domains and Subdomains:



Cybersecurity Governance	Cybersecurity Policies and Procedures Cybersecurity Roles and Responsibilities Cybersecurity Risk Management Cybersecurity in Industrial Control System Project Management Cybersecurity in Change Management Periodical Cybersecurity Review and Audit Cybersecurity in Human Resources Cybersecurity Awareness and Training Program
Cybersecurity Defense	Asset Management Identity and Access Management System and Processing Facility Protection Network Security Management Mobile Devices Security Data and Information Protection Cryptography Backup and Recovery Management Vulnerabilities Management Penetration Testing Cybersecurity Event Logs and Monitoring Management Cybersecurity Incident and Threat Management Physical Security
Cybersecurity Resilience	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Third-Party Cybersecurity	Third-Party Cybersecurity

Figure 3: OTCC Main Domains and Subdomains

Relationship Between OTCC and ECC Domain 5

The ECC Domain 5 “Industrial Control System Protection” includes controls and sub-controls for enhancing the cybersecurity level of OT/ICS environment in general. However, Operational Technology Cybersecurity Controls (OTCC-1:2022) specifies more detailed controls to increase the protection of OT/ICS systems.

Table (1) below illustrates the relationship between the cybersecurity controls stated in ECC domain 5 and the cybersecuirty controls stated in the OTCC document.

ECC Control ID	ECC Control Statement	Relation to OTCC Controls
5-1-1	Cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be defined, documented and approved.	1-1-1
5-1-2	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be implemented.	1-1-1
5-1-3	In addition to the applicable ECC controls from the main domains (1), (2), (3) and (4), the cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must include at least the following:	-
5-1-3-1	Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).	2-4-1-1, 2-4-1-2, 2-4-1-3, 2-4-1-6, 2-4-1-9, 2-4-1-10, 2-4-1-11, 2-4-1-12, 2-4-1-13
5-1-3-2	Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, wireless, remote access).	2-4-1-4, 2-4-1-5, 2-4-1-7, 2-4-1-8

5-1-3-3	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.	2-11-1, 2-11-3
5-1-3-4	Isolation of Safety Instrumental Systems (SIS).	2-4-1-3
5-1-3-5	Strict limitation on the use of external storage media.	2-3-1-8, 2-3-1-9
5-1-3-6	Strict limitation on connecting mobile devices to industrial production networks.	2-5-1-1, 2-5-1-2, 2-5-1-3, 2-5-1-4, 2-5-1-5
5-1-3-7	Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices.	2-3-1-1, 2-3-1-2, 2-3-1-3, 2-3-1-5, 2-3-1-7, 2-4-1-15
5-1-3-8	Vulnerability management for industrial control systems and operational technology (ICS/OT).	2-9-1-1, 2-9-1-2, 2-9-1-3,
5-1-3-9	Patch management for industrial control systems and operational technology (ICS/OT).	2-3-1-3, 2-5-1-2
5-1-3-10	Cybersecurity applications management related to the protection of the industrial systems from viruses and malware.	2-2-1-2, 2-3-1-1, 2-3-1-6, 2-11-1-5
5-1-4	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be reviewed periodically.	1-1-3, 1-4-2, 1-5-4, 1-7-2, 2-1-2, 2-2-2, 2-3-2, 2-4-2, 2-5-2, 2-6-2, 2-7-2, 2-8-2, 2-9-2, 2-10-2, 2-11-2, 2-12-2, 2-13-2, 3-1-2, 4-1-2

Table 1: Relationship Between OTCC and ECC Domain 5

Assigning OTCC Controls & Subcontrols Levels

Overview

This section provides a thorough process on how organizations assign appropriate levels to different facilities within their OT/ICS environment. Assigning the appropriate facility level must be based on the defined criteria to ensure appropriate controls are assigned to appropriate facilities.

Assigning Levels Approach

This approach consists of two main steps:

- Defining the criticality levels for facilities based on the results of Facility Level Identification Tool (OTCC-1:2022).
- Defining the applicable controls for each facility in accordance to the criticality of OT/ICS systems within the respective facility.

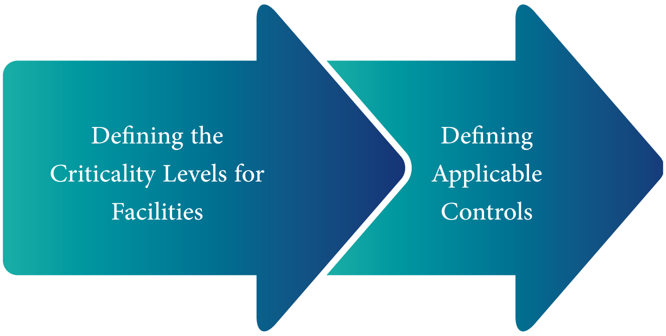

Defining the Criticality Levels for Facilities
Defining Applicable Controls

Figure 4: Main Steps to Apply Cybersecurity Controls in OT/ICS Environment

Defining the Criticality Levels for Facilities

There are three levels defined in the Operational Technology Cybersecurity Controls (OTCC) that are dependent on the criticality, consequences and impacts of the organization’s facilities containing OT/ICS systems or assets. This allows organizations to appropriately tailor its cybersecurity controls to its OT/ICS environment:

- **Level 1 (L1):** The criticality level of the facility is high and have severe adverse effects, consequences, and/or impacts to operations, catstrophic or assets, resources, or Health, Safety, and Environment (HSE) of the organization.
- **Level 2 (L2):** The criticality level of the facility is moderate and have significant effects, consequences, and/or impacts to operations, assets, resources, or Health, Safety, and Environment (HSE) of the organization.

- **Level 3 (L3):** The criticality level of the facility is low and have moderate adverse effects, consequences, and/or impacts to operations, assets, resources, or Health, Safety, and Environment (HSE) of the organization.

Each organization utilizes the Facility Level Identification Tool (OTCC-1:2022) when they identify the criticality level for their facilities based on the following criteria:

1. Negative impact to onsite and/or offsite population.
2. Negative environmental impact onsite and/or offsite areas.
3. Negative impact on national security.
4. Negative impact on the Kingdom's reputation and public image.
5. Unauthorized disclosure of data that is classified as Secret or Top Secret.
6. Disruption to the national economy.
7. Negative impact to a large number of beneficiaries.
8. National infrastructure interdependencies.
9. Facility interdependencies.

If an organizations owns industrial control systems with different criticality levels within the same facility, the criticality level of the facility will be based on the system with the highest criticality level.

Defining Applicable Controls

Once the organization has identified facilities' levels based on the defined criteria above, the organization shall comply with the applicable controls based on the results of the Facility Level Identification Tool. When the organization has different OT/ICS facilities that are separated and isolated, the levels can differ. Thus, the applicability of the controls will differ.

Each control and sub-control in OTCC document is associated with a specific level. The facility's level will determine the set of controls that must be applied to achieve compliance with OTCC document. Organizations that have facilities that are classified as L1 are required to implement all controls and subcontrols stated in the document. Organizations that have facilities that are classified as L2 are required to implement L2 and L3 controls. Organizations that have facilities that are classified as L3 are required to implement L3 controls at minimum. If a control or sub-control is not required to be applied based on the identified level, NCA encourages the organization to apply that control or sub-control.

International Standards Mapping to OTCC Controls

In case of a discrepancy between the OTCC document and the other national and international standards referenced in this document, the OTCC must take precedence.

1 Cybersecurity Governance

1-1	Cybersecurity Policies and Procedures							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-1-1	ORG 1.1, ORG 2.4	ZCR 6.1	-	ID.GV-1, ID.GV-2	PL-2	ISBR 8	003-R1, 003-R2	CPM-1, CPM-2c, CPM-2e, CPM-3b
1-1-2	CM 1.2	-	SR 7.6	PR.IP-3	CM-3, MA-1, SA-10	ISBR 6	002-R1, 002-R2, 003-R1, 003-R2	ACM-1c, ACM-2a,
1-1-3	ORG 1.6, ORG 2 (all)	ZCR 5.1, ZCR 6.6, ZCR 4.1, ZCR 7.1, ZCR 6.8	-	ID.GV-4, ID.RA-5, ID.BE (All), ID-GV-4, ID.RA-4	SA-11 (2), RA-3, PM-11, PL-2, PM-9	ISBR 13, ISBR 1, ISBR 2	002-R1, 002-R2, 003-R1, 003-R2	ISC-1 (all), CPM-2g RM-3e

1-2	Cybersecurity Roles and Responsibilities							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-2-1								
1-2-1-1	ORG 1.3, ORG 1.5	-	-	ID.AM-6, ID.GV-2, PR.AT-4	PS-1, PM-1, PM-2	ISBR 1, ISBR 3	002-R2, 003-R1, 003-R3, 003-R4	WM-1d, WM-1c
1-2-1-2	ORG 1.3, ORG 1.5	-	-	ID.AM-6, ID.GV-2, PR.AT-4	PS-1, PM-1, PM-2	ISBR 1, ISBR 3	002-R2, 003-R1, 003-R3, 003-R4	WM-1d, WM-1c

1-3	Cybersecurity Risk Management							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-3-1								
1-3-1-1	ORG 2.1	ZCR 3.3, ZCR 5.3, ZCR 7.1	-	ID.RM-1, ,ID.RM-3	RA-1, PM-1	ISBR 2	-	RM-3e

1-3-1-2	ORG 2.1, ORG 2.4, AVAIL 1.2, AVAIL 1.2, NET 1.5	ZCR 5.1, ZCR 5.3, ZCR 5.4, ZCR 5.5, ZCR 5.7, ZCR 5.10, ZCR 5.11, ZCR 5.13, ZCR 6.1, ZCR 6.6	-	ID.RA-4	RA-3, SA-11 (2), SA-15 (4), PM-16,	ISBR 5	002-R1, 008-R1	TVM-1d, TVM-1g, RM-2e, RM-1c
1-3-1-3	ORG 2.1	ZCR 5.13	-	ID.RA-6	RA-3	ISBR 2	-	-
1-3-1-4	ORG 2.1	ZCR 5.13	-	ID.GV-4	-	-	-	RM-2a, RM-1c
1-3-1-5	COMP 3.5	-	-	PR.IP-3	-	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	COMP 3.5
1-3-1-6	-	-	-	-	PL-8, PL-2	ISBR 6	-	CPM-3b,
1-3-1-7	-	-	-	-	PL-8, PL-2	ISBR 6	-	CPM-3b,
1-4	**Cybersecurity in Industrial Control System Project Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-4-1								
1-4-1-1	ORG 2.3, ORG 1.6	-	SR 3.3	ID.SC-4	CA-1, CM-4 (2) SA-1, SA-3, SA-4, SA-8, SA-11, SA-12	ISBR 8	-	CPM-4b
1-4-1-2	ORG 2.3, ORG 1.6	-	SR 7.6	-	-	ISBR 12	-	CPM-4b
1-4-1-3	-	-	-	PR.IP-9	CP-2 CP-3	-	-	-
1-4-1-4	-	-	-	ID.GV-4	PM-7	-	-	-
1-4-2	ORG 2.4	-	-	-	CM-7 (1)	ISBR 8	-	-
1-5	**Cybersecurity in Change Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-5-1	CM 1.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2	ACM-4a
1-5-2	CM 1.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2	ACM (all)
1-5-3								
1-5-3-1	CM 1.4	-	-	PR.IP-3	CM-4	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-3a
1-5-3-2	CM 1.4	-	-	PR.IP-3	CM-3(2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-4d

1-5-3-3	CM 1.4	-	-	PR.IP-3	IR-4 (2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	-
1-5-3-4	CM 1.4	-	-	PR.IP-3	IR-4 (2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	-
1-5-3-5	CM 1.4	-	SR 7.6 RE(1)	PR.IP-3	CM-2(2)	ISBR 10	010-R1, 010-R2	ACM-2d
1-5-4	CM 1.4, ORG 2.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-4g
1-6	**Periodical Cybersecurity Review and Audit**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-6-1	4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4	-	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	PR.PT-1	AU*	-	-	-
1-6-2	3.1.18	-	-	PR.PT-1	AU*	-	-	-
1-7	**Cybersecurity in Human Resources**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-7-1	USER 1.2, USER 1.4	-	-	-	PS-3	-	004-R3, 004-R4, 004-R5	WM-2a, WM-2c
1-7-2	-	-	-	PR.IP-11	PS-1	-	-	-
1-8	**Cybersecurity Awareness and Training Program**							
رقم الضابط	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
1-8-1	ORG 1.4	-	-	PR.AT-1, PR.AT-2, PR.AT-5	PR.AT-1	ISBR 5	004-R1, 004-R2	WM-3a, WM-3d
1-8-2								
1-8-2-1	ORG 1.5	-	-	PR.AT-2, PR.AT-5	PR-AT-3	ISBR 5	004-R1, 004-R2	WM-3i
1-8-2-2	ORG 1.5	-	-	PR.AT-2, PR.AT-5	PR-AT-3	ISBR 5	004-R1, 004-R2	WM-3i

2 Cybersecurity Defense

2-1 Asset Management

OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-1-1								
2-1-1-1	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
2-1-1-2	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
2-1-1-3	AVAIL 2.4, USER 1.5	-	SR 2.1 RE(1), SR 7.7	PR.AC-4	CP-9 (3), CM-8 (7)	ISBR 17	002-R2, 003-R1, 003-R2	-
2-1-1-4	ORG 1.3	-	SR 2.1	ID.GV-2	CM-9 (1)	ISBR 3	002-R2	-
2-1-1-5	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
2-1-2	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-

2-2 Identity and Access Management

OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-2-1								
2-2-1-1	-	-	SR 1.1, SR 2.1	-	-	-	007-R5	-
2-2-1-2	USER 1.2	-	SR 1.2	PR.AC-7	AC-2 (1)	ISBR 19	007-R5	IAM-1a
2-2-1-3	USER 1.2	-	SR 1.2	PR.AC-1	AC-2 (2)	ISBR 19	007-R5	IAM-1c
2-2-1-4	USER 1.16	-	SR 2.5, SR 2.6	-	AC-11, AC-12, SI-14	-	003-R1, 005-R1, 005-R2	-
2-2-1-5	-	-	-	-	AC-2 (1)	ISBR 19	-	-
2-2-1-6	USER 2.3, USER 2.4	-	SR 2.1 RE(3), SR 2.1 RE(4)	-	AC-3 (2)	ISBR 19	007-R5	-
2-2-1-7	NET 1.1	ZCR 2.1, 3.1, 4.1	SR 5.2	PR.AC-3	SC-1, SC-7	ISBR 4	005-R2	CPM-3 (all)
2-2-1-8	USER 1.2	-	SR 1.4	PR.AC-1	IA-5	-	007-R5	IAM-1a
2-2-1-9	DATA 1.2	-	SR 1.7	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-
2-2-1-10	-	-	SR 4.1 RE(1)	PR.AC-1	-	ISBR 19	007-R5, 010-R1	IAM-1d

2-2-1-11	USER 1.2	-	-	PR.AC-1	AC-2 (2)	ISBR 19	007-R5	IAM-1c
2-2-2	USER 1.2	-	SR 1.2	R.AC-1	-	-	-	-
2-3	**System and Processing Facilities Protection**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-1-1								
2-3-1-1	COMP 1.1, COMP 2.2	-	SR 3.2, SR 5.2	DE.CM-4	SI-3	ISBR 13	007-R3, 007-R4, 010-R1, 010-R2	SA-2b, SA-2e, SA-2j
2-3-1-2	COMP 1.1, USER 1.5, COMP 3	-	-	PR.PT-3	CM-6, CM-7	ISBR 6	007-R2	TVM-2c
2-3-1-3	COMP 1.1, USER 1.5, COMP 3	-	-	PR.PT-3	CM-6, CM-7	ISBR 6	007-R2	TVM-2c
2-3-1-4	-	-	SR 7.7	PR.IP-1	CM-7	-	-	-
2-3-1-5	DATA 1.3	-	SR 5.2 RE(3)	-	AU-5 (4), CP-12	-	010-R1, 010-R2	-
2-3-1-6	-	-	SR 7.7 SR 3.2	PR.IP-1	CM-7	-	-	-
2-3-1-7	NET 1.3, COMP 1.1, COMP 3.3, EVENT 1.1, EVENT 1.5	ZCR 3.1, ZCR 3.3	SR 5.1 RE(3), SR 2.1 RE(1)	PR.IP-3, PR.AC-4	SA-17 (7)	ISBR 6	005-R1, 010-R1, 010-R2	SA-4a, IAM-2d,
2-3-1-8	COMP 1.2, COMP 2.1	-	SR 3.2 RE(1)	PR.PT-2, DE.CM-4	MA-3 (2), MP (all)	ISBR 13	004-R2, 007-R1, 007-R3, 007-R4, 010-R4	IAM-1a, IAM-2a
2-3-1-9	COMP 1.2, COMP 2.1	-	SR 3.2 RE(1)	PR.PT-2, DE.CM-4	MA-3 (2), MP (all)	ISBR 13	004-R2, 007-R1, 007-R3, 007-R4, 010-R4	IAM-1a, IAM-2a
2-3-1-10	-	-	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	PR.PT-1	AU-1*	-	001-R4 002-R4 003-R4	-
2-3-1-11	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2d
2-3-1-12	ORG 2.2	-	SR 2.8	DE.AE-7	CA-7	ISBR 13	007-R4	SA-2b
2-3-1-13	EVENT 1.7	-	SR 2.8 RE(1)	DE.AE-3	AU-6 (4)	ISBR 2	007-R4	SA-1c, SA-1e
2-3-2	COMP 1.1, COMP 2.2	-	SR 3.2, SR 5.2	DE.CM-4	SI-3	ISBR 13	007-R3, 007-R4, 010-R1, 010-R2	SA-2b, SA-2e, SA-2j

2-4	Network Security Management							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-4-1								
2-4-1-1	NET 1.1	-	SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	AC-17, SC-7	ISBR 4	005-R1, 006-R1	SA-2b, SA-2e, SA-2j
2-4-1-2	NET 1.1, NET 1.3	ZCR 3.2	SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	SC-7	ISBR 4	005-R1, 006-R1	CPM-3 (all)
2-4-1-3	NET 1.3	ZCR 3.3	SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	SC-7	ISBR 4	002-R1, 005-R1, 006-R1	CPM-3 (all)
2-4-1-4	NET 2 (ALL)	ZCR 3.5	SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	AC-18 (all), SI-4 (14)	ISBR 4	-	CPM-3 (all)
2-4-1-5	NET 2.2, NET 1.6	ZCR 3.5	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	AC-18 (all)	ISBR 4	-	CPM-3 (all)
2-4-1-6	NET 1.7	ZCR 3.6	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-5	MA-4 (4), SC-7 (5)	ISBR 4	005-R1, 007-R1	CPM-3 (all)
2-4-1-7	USER 1.16	-	SR 2.5, SR 2.6	-	AC-11, AC-12, SI-14	-	003-R1, 005-R1, 005-R2	CPM-3 (all)
2-4-1-8	NET 3 (ALL)	-	SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7	ISBR 4	005-R1	-
2-4-1-9	NET 3 (ALL)	ZCR 3.2	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7, SC-7 (8)	ISBR 4	005-R2	CPM-3 (all)
2-4-1-10	NET 3 (ALL)	ZCR 3.2	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7, SC-7 (8)	ISBR 4	005-R2	CPM-3 (all)
2-4-1-11	NET 3 (ALL)	ZCR 3.2	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7, SC-7 (8)	ISBR 4	005-R2	CPM-3 (all)
2-4-1-12	NET 3 (ALL)	ZCR 3.2	SR 1.6, SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7, SC-7 (8)	ISBR 4	005-R2	CPM-3 (all)
2-4-1-13	NET 3 (ALL)	-	SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7	ISBR 4	005-R1	CPM-3 (all)
2-4-1-14	NET 3 (ALL)	-	SR 5.1 (all), SR 5.2 (all)	PR.AC-3, PR.AC-5, PR.PT-4	MA-4 (4), SC-7	ISBR 4	005-R1	CPM-3 (all)

2-4-1-15	NET 1.2	ZCR 6.3	-	ID.AM-3, DE.AE-1	CA-9, SI-4, CA-3	ISBR 11	005-R1	CPM-3 (all)
2-4-1-16	NET 1.2	ZCR 6.3	-	ID.AM-3, DE.AE-1	CA-9, SI-4, CA-3	ISBR 11	005-R1	CPM-3 (all)
2-4-2	NET 1.1	-	SR 5.1 (all), SR 5.2 (all)	PR.AC-5, PR.PT-4	AC-17, SC-7	ISBR 4	005-R1, 006-R1	CPM-3 (all)
2-5	**Mobile Devices Security**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-5-1								
2-5-1-1	-	-	SR 2.3	PR.AC-7	ISBR 6	ISBR 4	007-R3, 007-R4, 010-R3, 010-R4	-
2-5-1-2	NET 2 (all), NET 1.7, NET 1.8 COMP 1.2, COMP 2.1	-	SR 2.3 (all), SR 2.2, SR 2.2 RE(1)	PR.AC-7, ,DE.CM-7	ISBR 6	ISBR 6 ISBR 13	007-R3, 007-R4, 010-R3, 010-R5 010-R6	-
2-5-1-3	-	-	SR 2.3	PR.AC-3	AC-19	ISBR 6	-	-
2-5-1-4	-	-	SR 2.3	-	AC-19	ISBR 6	-	-
2-5-1-5	-	-	SR 4.2	-	AC-19	ISBR 6	-	-
2-5-2	NET 2 (all), NET 1.7, NET 1.8 COMP 1.2, COMP 2.1	-	SR 2.3	PR.AC-7	AC-19	ISBR 6	007-R3, 007-R4, 010-R3, 010-R4	-
2-6	**Data and Information Protection**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-6-1								
2-6-1-1	DATA 1.2	-	SR 4.1 RE(1)	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-
2-6-1-2	-	-	SR 3.4 SR 4.1	PR.DS-1, PR.DS-2	-	-	-	-
2-6-1-3	DATA 1.6	-	SR 4.2 (all)	ID.GV-4	MP-6	-	011-R1, 011-R2	-
2-6-1-4	,4.3.3.3.9 4.3.4.4.1	-	SR 4.2	PR.DS-7 PR.DS-3	CM-8, MP-6, PE-16 CM-2	-	-	-
2-6-2	DATA 1.2	-	SR 4.1 , 4.2	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-
2-7	**Cryptography**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1

2-7-1	DATA 1.7	-	SR 3.1 (all), SR 4.1 (all), SR 4.3	PR.DS-1, PR.DS-2	SC-13	-	-	-
2-7-2	DATA 1.7	-	SR 3.1 (all), SR 4.1 (all), SR 4.3	PR.DS-1, PR.DS-2	SC-13	-	-	-
2-8	**Backup and Recovery Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-8-1								
2-8-1-1	AVAIL 2.4	-	-	PR.IP-4	CP-9 (3)	ISBR 15	009-R1	-
2-8-1-2	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-9	ISBR 17	009-R1	-
2-8-1-3	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-9	ISBR 17	009-R1	-
2-8-1-4	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-6	-	009-R1	-
2-8-2	AVAIL 2.4	-	-	PR.IP-4	CP-9 (3)	ISBR 15	009-R1	-
2-9	**Vulnerabilities Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-9-1								
2-9-1-1	ORG 2.2, EVENT 1.9	ZCR 5.13	-	ID.RA-1, PR.IP-12	RA-3, RA-5	ISBR 6, ISBR 10, ISBR 12	010-R3	TVM-2 (all)
2-9-1-2	EVENT 1.9	ZCR 5.13	SR 3.3	PR.IP-12	CA-5	ISBR 13	010-R3	TVM-2f
2-9-1-3	ORG 2.1	-	-	-	RA-5	-	003-R1, 010-R3	-
2-9-2	EVENT 1.9	ZCR 5.13	SR 3.3	PR.IP-12	CA-5	ISBR 13	010-R3	TVM-2f
2-10	**Penetration Testing**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-10-1								
2-10-1-1	-	-	-	-	CA-8	-	010-R2	TVM-2e
2-10-1-2	-	-	-	-	CA-8	-	-	TVM-2e
2-10-1-3	-	-	-	-	CA-8	-	010-R2	TVM-2e
2-10-1-4	-	-	-	-	CA-8	-	010-R2	TVM-2e
2-10-2	-	-	-	-	CA-8	-	010-R2	TVM-2e
2-11	**Cybersecurity Event Logs and Monitoring Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1

2-11-1								
2-11-1-1	EVENT 1.1, EVENT 1.2, EVENT 1.5	-	SR 2.8, SR 6.1	PR.PT-1, DE.AE-3, DE.CM-1	AU-2	ISBR 16	007-R4	SA-1a, SA-1b
2-11-1-2	-	-	SR 2.10	DE.DP-3	AU-5	-	007-R4	-
2-11-1-3	EVENT 1.7	-	SR 6.2	DE.AE-2	CA-7	ISBR 2	007-R4	SA-2a
2-11-1-4	-	SR 2.8	DE.CM-3	CA-7	ISBR 13	007-R4	SA-2b	-
2-11-1-5	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2d
2-11-1-6	ORG 2.2	-	SR 2.8	DE.CM-7	CA-7	ISBR 13	010-R2	SA-2b
2-11-1-7	ORG 2.2	-	SR 2.8	DE.CM-7	SI-4	ISBR 18	005-R2	SA-2b
2-11-1-8	EVENT 1.1, EVENT 1.2, EVENT 1.5	-	SR 2.8, SR 6.1	PR.PT-1, DE.AE-3, DE.CM-1	AU-2	ISBR 16	007-R4	SA-1a, SA-1b
2-11-1-9	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2b
2-11-1-10	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2b
2-11-2	EVENT 1.1, EVENT 1.2, EVENT 1.5	-	SR 2.8, SR 6.1	PR.PT-1, DE.AE-3, DE.CM-1	AU-2	ISBR 16	007-R4	SA-1a, SA-1b
2-12	**Cybersecurity Incident and Threat Management**							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-12-1								
2-12-1-1	EVENT 1.8	-	-	RS.RP (all)	IR-1, IR-8	ISBR 16	008-R1, 008-R2, 008-R3	IR-3f
2-12-1-2	EVENT 1.7	-	-	RS.AN-2, RS.AN-3	IR-4	ISBR 16	008-R3	IR-3h
2-12-1-3	EVENT 1.8, AVAIL 2.5	-	-	RS.RP (all)	IR-4, IR-1	ISBR 15	009-R1, 009-R2, 009-R3	IR-4b
2-12-1-4	EVENT 1.8	-	-	RS.CO (all)	IR-8	ISBR 16	008-R1, 009-R1	IR-3c
2-12-1-5	-	-	-	-	-	-	008-R1, 008-R2, 008-R3	IR-4c
2-12-1-6	ORG 2.3	-	-	PR.IP-2	CM-9, SA-3, SA-4 (3), SA-8, SA-15	-	-	EDM-2e, CPM-2f, CPM-4b
2-12-1-7	-	-	SR 3.3	PR.IP-10	IR-3	-	-	-
2-12-1-8	-	ZCR 5.1, ZCR 6.6	-	ID.RA-2	SA-12 (8)	ISBR 5, ISBR 13	-	TVM-1a, TVM-1e, TVM-1f, TVM-1j
2-12-2	EVENT 1.8	-	-	RS.RP (all)	IR-1, IR-8	ISBR 16	008-R1, 008-R2, 008-R3	TVM-1a, TVM-1e, TVM-1f, TVM-1j

2-13	Physical Security							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-13-1								
2-13-1-1	ORG 3.1	-	-	DE.CM-7	PE-2	-	-	-
2-13-1-2	ORG 3.1	-	-	DE.CM-7	PE-3	-	-	-
2-13-1-3	ORG 3.1	-	-	DE.CM-7	PE-3	-	-	-
2-13-1-4	ORG 3.1	-	-	DE.CM-7	PE-6, PE-6, PE-6 (1), PE-6 (3), PE-6 (4)	-	006-R1	-
2-13-1-5	ORG 3.1	-	-	-	-	-	-	-
2-13-1-6	ORG 3.1	-	-	-	PE-8	-	-	-
2-13-1-7	-	-	-	DE.CM-6	MA-2	-	-	-
2-13-1-8	ORG 3.1	-	-	PR.AT-5	AT-2 PM-13	-	-	-
2-13-1-9	ORG 3.1	-	-	PR.AT-5	AT-2 PM-13	-	-	-
2-13-2	-	-	-	-	PE-1	-	-	-

3 Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
3-1-1								
3-1-1-1	AVAIL 2.1	-	SR7.4	PR.IP-4	CP-9	ISBR 9	009-R1	IR-4c
3-1-1-2	AVAIL 1.1, AVAIL 1.2	-	SR 7.2, SR 7.3	PR.IP-4, PR.DS-4	CP-9 (6), PE-9 (1)	-	005-R1, 006-R1, 009-R1	IR-4c
3-1-1-3	AVAIL 1.1	-	-	PR.IP-9	PR.IP-9, CP-2 (5)	-	009-R1	IR-4c, IR-4e, IR-4h
3-1-1-4	AVAIL 1.1	ZCR 5.3, ZCR 5.4	SR 7.4	PR.IP-9	CP-6, CP-6 (1), CP-6 (2), CP-6 (3), CP-7, CP-7 (1), CP-7 (2), CP-7 (3), (CP-7 (4	ISBR 7	009-R1, 009-R2, 009-R3	IR-2a, IR-2d, IR-4a
3-1-1-5	AVAIL 1.2	-	SR 7.4, SR 7.5	PR.PT-5, PR.DS-4	SI-13 (4), (SI-13 (5	-	002-R1, 008-R2, 009-R2	-
3-1-1-6	-	-	-	PR.IP-10	CP-3 (1), CP-3 (2), CP-4 (3)	-	008-R2, 009-R2	-
3-1-2	AVAIL 2.1	-	SR7.4	PR.IP-4	CP-9	ISBR 9	009-R1	IR-4c

4 Third-Party Cybersecurity

4-1	Third-Party Cybersecurity							
OTCC Control ID	Standards							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
4-1-1								
4-1-1-1	ORG 1.6	ZCR 5.12	-	ID.SC-1, ID.SC-3	SA-12	ISBR 8	013-R1, 013-R2	-
4-1-1-2	ORG 1.6	-	-	ID.SC-2	IR-6 (3), PS-7, UL-2	-	013-R1, 013-R2	-
4-1-1-3	ORG 2.3	-	-	PR.IP-2	CM-9, SA-3, SA-4 (3), SA-8, SA-15	-	-	EDM-2e, CPM-2f, CPM-4b
4-1-1-4	-	-	SR 6.1	ID.SC-4	-	-	-	-
4-1-2	ID.SC-1	-	SR 6.1	ID.SC-4	-	-	-	-

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority