NIST Interagency Report
NIST IR 8406 ipd

Cybersecurity Framework Profile for Liquefied Natural Gas

Initial Public Draft

William Newhouse
Josephine Long
David Weitzel
Jason Warren
Michael Thompson
Chris Yates
Hillary Tran
Alicia Mink
Aurora Herriott
Tom Cottle

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Cybersecurity Framework Profile for Liquefied Natural Gas

Initial Public Draft

William Newhouse
Applied Cybersecurity Division / National
Cybersecurity Center of Excellence
Information Technology Laboratory

Josephine Long
David Weitzel
Jason Warren
Michael Thompson
Chris Yates
Hillary Tran
Alicia Mink
Aurora Herriott
Tom Cottle
The MITRE Corporation
McLean, VA

37 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
38 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
39 endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the
40 entities, materials, or equipment are necessarily the best available for the purpose.

41 There may be references in this publication to other publications currently under development by NIST in
42 accordance with its assigned statutory responsibilities. The information in this publication, including concepts and
43 methodologies, may be used by federal agencies even before the completion of such companion publications. Thus,
44 until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain
45 operative. For planning and transition purposes, federal agencies may wish to closely follow the development of
46 these new publications by NIST.

47 Organizations are encouraged to review all draft publications during public comment periods and provide feedback
48 to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
49 https://csrc.nist.gov/publications.

50 **NIST Technical Series Policies**

51 Copyright, Fair Use, and Licensing Statements
52 NIST Technical Series Publication Identifier Syntax

53 **How to Cite this NIST Technical Series Publication:**

57 **Author ORCID iDs**

58 William Newhouse: 0000-0002-4873-7648

59 **Public Comment Period**

60 October 17, 2022 – November 17, 2022

61 **Submit Comments**

62 LNG-CSF-Profile-NCCoE@nist.gov
63
64 National Institute of Standards and Technology
65 Attn: National Cybersecurity Center of Excellence, Applied Cybersecurity Division, Information Technology
66 Laboratory
67 100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

68 **All comments are subject to release under the Freedom of Information Act (FOIA).**

Abstract

This document is the Cybersecurity Framework Profile developed for the Liquefied Natural Gas (LNG) industry and the subsidiary functions that support the overarching liquefaction process, transport, and distribution of LNG. The LNG Cybersecurity Framework Profile can be used by liquefaction facilities, LNG vessels, and other supporting entities of the LNG lifecycle so that cybersecurity risks associated with these critical processes and systems can be minimized. The LNG Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to the overall LNG process. The Cybersecurity Framework LNG Profile is meant to supplement but not replace current cybersecurity standards, regulations, and industry guidelines that are already being used by the Liquefied Natural Gas industry.

Keywords

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

  i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

  ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: LNG-CSF-Profile-NCCoE@nist.gov with the subject "NISTIR 8406 call for patent claims".

118 **Table of Contents**

List of Tables

201   **List of Figures**

Acknowledgments

The authors gratefully acknowledge and appreciate the following contributors for their keen, insightful, and dedicated assistance with developing this document:

U.S. DEPARTMENT OF ENERGY

226 **1. Introduction**

227 The NIST Cybersecurity Framework (CSF) [1] is a voluntary, risk-based assemblage of industry
228 standards and best practices designed to help organizations manage cybersecurity risks. The
229 CSF, created through a collaborative public process, uses a common language to address and
230 manage cybersecurity risk in a cost-effective way based on business needs without imposing
231 additional regulatory requirements. Although the CSF presents a variety of mitigations, many
232 sectors and industries have opted to create their own prioritizations, known as CSF Profiles
233 ("Profile"). This document is one such Profile, an application of the CSF to LNG industry.

234 Today, oil and natural gas make up 55 percent of the global energy use, and the United States is
235 the world's largest producer of natural gas. Natural gas is a vital energy source for the U.S.,
236 supplying nearly one-third of the United States' primary energy and serving as the primary
237 heating fuel for approximately half of U.S. households [2]. While most natural gas is delivered in
238 its gaseous form via pipeline in the United States, the international market's growing need for
239 natural gas has given rise to its use in a liquefied form, or LNG. The international market for
240 LNG relies on safe handling of this energy resource within the U.S. Marine Transportation
241 System (MTS).

242 **1.1. Purpose and Scope**

243 To help jurisdictions across the United States safeguard LNG, this Profile is written around high-
244 level, mission-oriented goals ("mission objectives") of LNG infrastructure as identified by
245 industry stakeholders who were listed as contributors on the previous page. These Mission
246 objectives, described in Sec. 5, do not directly address every technical aspect of the LNG
247 process. Specifically, technical components of LNG systems necessary for accomplishing those
248 goals vary widely across the United States and cannot be captured in their entirety within a single
249 Profile. This Profile will help the LNG sector focus on the functions that require attention and
250 allow sector stakeholders to implement specific controls that are most suitable for their set of
251 circumstances.

252 This Profile can help organizations identify opportunities for managing cybersecurity risks in the
253 LNG lifecycle. Section 5 of this document provides a baseline of the Mission objectives for LNG
254 operations that were identified and prioritized by LNG industry stakeholders. Section 6 builds on
255 the identified Mission objectives to develop a prioritized list of CSF Categories. Section 7 of this
256 document includes a table of prioritized CSF Subcategories based on identified CSF Categories.
257 These prioritizations of Mission objectives, CSF Categories, and CSF Subcategories may serve
258 as a useful starting point to identify cybersecurity activities and outcomes that may be important
259 to members of the LNG industry. Additionally, prioritizations can be tailored to account for
260 specific mission objectives or operational considerations. A similar method to that described in
261 Sec. 4 can be applied to tailor this Profile for an individual organization.

262 Organizations across the energy sector place a high priority on mitigating risks to operational
263 technologies (OT)—the systems used to monitor and control physical processes. These systems
264 manage critical energy sector processes that, if damaged or disrupted, could impact energy
265 delivery, public safety, and national security. This Profile focuses on managing risks to OT
266 systems in LNG operations, including onboard monitoring and control technologies and remotely

267 managed, third-party systems. In addition to the recommendations for LNG organizations
268 offered in this Profile, additional high-level OT-specific issues should be considered when
269 reviewing this Profile and the CSF. OT environments typically encompass expansive and diverse
270 assets that may not be controllable through conventional information technology (IT)-based
271 cybersecurity tools, techniques, and methods due to the design and architecture of some OT
272 assets. These assets also have a high potential for operational disruption when cybersecurity
273 monitoring or scanning tools are applied to OT environments. Implementing separate-but-
274 connected IT and OT networks is an effective way to mitigate various risks, including the impact
275 that tools designed for IT networks may have on OT assets. Organizations may also face
276 additional supply chain-related challenges as many field assets are vendor-supplied and
277 operational needs may drive acquisition decisions. Procurement and change management
278 processes that engage engineering and IT stakeholders can help to mitigate some of this risk.
279 Given that OT assets drive core business processes for LNG organizations, additional
280 consideration can be given to these issues when applying the guidance in this Profile.

281 This document is not intended to replace any existing cybersecurity guidance or policy, but
282 rather to complement existing best practices by helping stakeholders prioritize the
283 recommendations provided by LNG organizations such as Shell, Exxon Mobil, Kinder Morgan,
284 Golden Pass, and Cheniere. Organizations face unique risks, and therefore a sector-wide Profile
285 does not guarantee protection from all cyber threats. The decision on how to implement the
286 Profile should be based on an organization's risk tolerance, environment, and operational needs.

1.1. Audience

288 This document is intended for those within the LNG industry who seek a greater understanding
289 of cybersecurity risks to the Liquefied Natural Gas Industry.

290 This document can also serve as a guide to those who need to create a Profile for their own
291 organization.

292 LNG processes are complex and varied, so some knowledge of the Marine Transportation
293 System (MTS) and the liquefaction process will be helpful to readers. An understanding of
294 cybersecurity concepts will also be useful for those managing, implementing, and maintaining
295 LNG systems impacted by this Profile.

1.2. Document Structure

297 This document consists of the following sections:

298 • Section 2 provides an overview of the LNG industry.
299 • Section 3 discusses key aspects of the CSF and CSF Profiles.
300 • Section 4 describes the methodology used to develop this Profile.
301 • Section 5 presents the high-level Mission objectives that support the LNG industry.
302 • Section 6 summarizes CSF Categories prioritized for the LNG industry.
303 • Section 7 details the relative importance of CSF Subcategories to the LNG industry.
304 • A References section contains a list of all items cited in this document.
305 • Appendix A defines acronyms used in this document.
306 • Appendix B provides a glossary of key terms used in this document.

2. The Liquefied Natural Gas Industry

This publication was prepared for the U.S. Department of Energy's CESER as part of an inter-agency agreement with NIST's National Cybersecurity Center of Excellence (NCCoE) to research and develop tools and practices that will strengthen the cybersecurity of the systems that handle energy resources within our nation's MTS. This Profile is focused on the LNG energy resource. CESER and NIST's NCCOE developed this Profile through a collaborative process, driven by LNG asset owners and operators.

2.1. The Need for Liquefied Natural Gas

Liquefying natural gas is a method used to convey it long distances when pipeline transport is not available or feasible. Specifically, LNG allows markets that are too far away from producing regions and connections to natural gas pipelines to gain access to natural gas. In its compacted liquid form, natural gas can be shipped in specialized LNG vessels to terminals around the world. For LNG to stay in its liquid state, it must be kept at about -260° Fahrenheit—for shipping and storage. The volume of natural gas in its liquid state is about 600 times smaller than its volume in its gaseous state [3]. This process makes it possible to transport natural gas to places pipelines are unable to reach. At ports with terminals for receiving LNG, the LNG is returned to its gaseous state and transported by pipeline to distribution companies, industrial consumers, and power plants.

2.2. Liquefied Natural Gas Safety

Due to comprehensive safety and security programs prescribed for LNG vessels and receiving terminals, more than 33,000 shipments have transported more than three billion cubic meters of LNG without a serious accident at sea or in port in the past 40 years [4]. LNG facilities and vessels feature state-of-the-art natural gas-, fire-, and smoke-detection systems that identify hazardous situations, and automatic shutdown systems that can halt operations. In the U.S., security measures for the waterfront portions of marine terminals and LNG vessels are regulated by the U.S. Coast Guard, whose responsibilities include keeping other ships from getting near LNG vessels while in transit or docked at an LNG port facility [5]. The Federal Energy Regulatory Commission also serves as a coordinator with the Coast Guard and other agencies on issues of marine safety and security at LNG import facilities [6].

2.3. Components of the Liquefied Natural Gas Industry

Components of the Liquefied Natural Gas industry are very complex, are often automated, and require considerable effort and coordination when an organization seeks alignment of standards, guidelines, and practices to identify opportunities for improving their cybersecurity posture.

Figure 1 shows the components of the Liquefied Natural Gas industry supply chain main components. The remainder of this section will focus on the following components of that supply chain:

- Liquefaction Facilities
- LNG Vessels and the Marine Transportation System (MTS)

345   • LNG Port Facilities
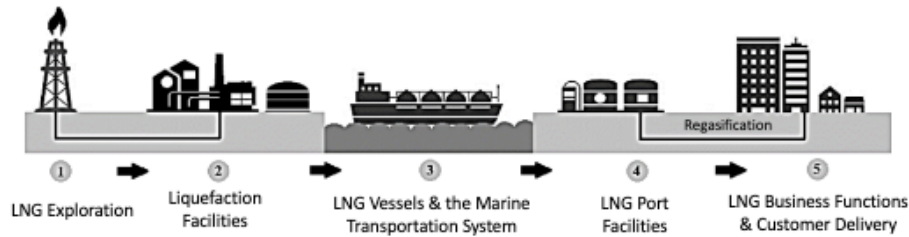
Fig. 1. Liquefied Natural Gas Industry Supply Chain Main Components

2.3.1. Liquefaction Facilities

LNG liquefaction facilities are used for converting, transporting, or storing LNG. The LNG facility is responsible for extracting unprocessed natural gas from reservoirs, on-site processing, and bringing the gas to a treatment facility. When brought to the treatment facility or liquefaction plant, the gas is then processed and treated through the gas liquefaction cycle before storage and transportation.

2.3.1.1.   Critical Systems Found in LNG Liquefaction Facilities

- **Gas Pre-Treatment (Pre-Liquefaction)**
  Prior to liquefaction, it is essential to begin the process with a pre-treatment. The gas pre-treatment removes impurities, such as any non-methane chemicals, from the natural gas stream. This pre-treatment prepares the gas for liquefaction and reduces the chance of hydrates forming, which will hinder the performance of operations.

- **Liquefaction**
  The liquefaction process is what turns the natural gas into Liquefied Natural Gas. Following the pre-treatment, the natural gas is sent to a heat exchanger where a mixed refrigerant is compressed and allowed to expand using a Joule-Thomson (JT) Valve. The change in temperature that accompanies expansion of a gas without production of work or transfer of heat is the Joule-Thomson effect, which results in the change in states of matter—liquefied gases. The key mechanical components are the JT valves and compressors, while the control system components include the programmable logic controller (PLC), instrumentation, and operator Human-Machine Interfaces (HMI).

- **Liquefied Natural Gas Storage**
  LNG is a cryogen and is kept in a liquid state within transfer and storage systems. Temperature within the tank will remain constant if the pressure is kept consistent by allowing the boil-off gas (BOG) to escape from the tank, which is known as auto-refrigeration. During this process, mechanical components include pumps, valves, and tanks, along with the BOG system. Control system components include PLC, instrumentation, and operator HMI.

375 ### 2.3.2. Liquefied Natural Gas Vessels and the Marine Transportation System

376 In the United States, the MTS encompasses ports, terminals, vessels, related infrastructure, and
377 mariners or operators. The MTS is diverse and dynamic, made of 25,000 miles of navigable
378 channels, 250 locks, 3,600 marine terminals, and 174,000 miles of railway [7]. The MTS consists
379 of waterways, ports, and intermodal landside connections that allow various modes of
380 transportation to move people and goods to, from, and on the water. Freight transport by sea has
381 been widely utilized in the MTS.

382 LNG vessels are specialized tank ships that must meet high international and U.S. Coast Guard
383 standards. These are high-tech vessels that use special materials and designs to safely handle the
384 very cold LNG. The enterprise resource planning system and an integrated automation system
385 manage OT systems on an LNG tank ship. These systems incorporate human-machine interface
386 that monitor process data and can access trend data or messages. Decision support tools, such as
387 Bridge Systems and Navigation Systems, contribute to the safety and reliability of shipping
388 operations.

389 ### 2.3.3. Liquefied Port Facilities

390 An LNG export terminal is a facility built specifically to receive the natural gas, liquefy it, store
391 the LNG, and transfer the LNG to ships for export.

392 An LNG import terminal reverses this process, receiving imported LNG from ships, storing it as
393 needed, regasifying the LNG back to natural gas, and distributing the natural gas via pipelines to
394 customers. LNG import terminals are typically located close to cities or dense populations for
395 accessible distribution and trade of natural gas.

396 LNG export and import terminals can be further described as being one of two types, deep water
397 port terminals located outside State waters and terminals located on the coastline or within State
398 waters.

399 ## 3. Overview of the Cybersecurity Framework

400 The CSF [1] uses business drivers to guide cybersecurity activities within an organization. The
401 CSF enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity
402 sophistication—to apply the principles and best practices of risk management to improving
403 security and resilience. It provides a common language for understanding, managing, and
404 expressing cybersecurity risk and cybersecurity management communications among internal
405 and external stakeholders and across an organization, regardless of cybersecurity expertise. For
406 organizations that require a starting point for leveraging the CSF, NIST's Getting Started with
407 the NIST Cybersecurity Framework: A Quick Start Guide provides an overview and explanation
408 for each of the CSF Functions [8].

409 The CSF consists of three main components: the Core, Profiles, and Implementation Tiers. The
410 Core is a catalog of desired cybersecurity activities and outcomes using common language that is
411 easy to understand. A CSF profile is an alignment of organizational requirements, objectives,
412 risk appetite, and resources against the desired outcomes of the CSF Core. Profiles are primarily
413 used to identify and prioritize opportunities for improving cybersecurity at an organization.
414 Implementation Tiers guide organizations to consider the appropriate level of rigor for their

415   cybersecurity program and can be used as a communication tool to discuss risk appetite, mission
416   priority, and budget. (Although part of the CSF, for the purposes of this Profile further discussion
417   on Implementation Tiers is not included.)

418   ## 3.1.   The Cybersecurity Framework Core

419   The CSF presents industry standards, guidelines, and practices in a manner that allows for
420   communication of cybersecurity activities and outcomes across the organization, including
421   executive leadership and those responsible for operations. The CSF Core consists of five
422   concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When
423   considered together, these Functions provide a high-level, strategic view for cybersecurity risk
424   management of an organization's cybersecurity posture. The CSF further identifies underlying
425   key Categories and Subcategories for each Function and matches them with example Informative
426   References, such as existing standards, guidelines, and practices for each Subcategory. The five
427   Functions include 23 Categories of cybersecurity outcomes and Subcategories that further divide
428   the Categories into more specific technical or management activities. The 23 Categories are
429   spread across the Functions named in Table 1.

430   The five Functions of the CSF Core are defined below:

431   - **Identify** – Develop the organizational understanding to manage cybersecurity risk to
432   systems, assets, data, and capabilities. The activities in the Identify Function are
433   foundational for effective use of the CSF. Understanding the business context, the
434   resources that support critical functions, and the related cybersecurity risks enables an
435   organization to focus and prioritize its efforts, consistent with its risk management
436   strategy and business needs. Examples of outcome Categories within this Function
437   include Asset Management, Business Environment, Governance, Risk Assessment, and
438   Risk Management Strategy.

439   - **Protect** – Develop and implement the appropriate safeguards to ensure delivery of
440   critical infrastructure services. The activities in the Protect Function support the ability to
441   limit or contain the impact of a potential cybersecurity event. Examples of outcome
442   Categories within this Function include Identity Management and Access Control,
443   Awareness and Training, Data Security; Information Protection Processes and
444   Procedures, Maintenance; and Protective Technology.

445   - **Detect** – Develop and implement the appropriate activities to identify the occurrence of a
446   cybersecurity event. The activities in the Detect Function enable timely discovery of
447   cybersecurity events. Examples of outcome Categories within this Function include
448   Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

449   - **Respond** – Develop and implement the appropriate activities to act on a detected
450   cybersecurity event. The activities in the Respond Function support the ability to contain
451   the impact of a potential cybersecurity event. Examples of outcome Categories within
452   this Function include Response Planning, Communications, Analysis, Mitigation, and
453   Improvements.

454 • **Recover** – Develop and implement the appropriate activities to maintain plans for
455 resilience and to restore any capabilities or services that were impaired due to a
456 cybersecurity event. The activities in the Recover Function support timely recovery to
457 normal operations to reduce the impact from a cybersecurity event. Examples of outcome
458 Categories within this Function include Recovery Planning, Improvements, and
459 Communications.

460 **Table 1.** Cybersecurity Framework Functions and Categories.

Function	Function Unique Identifier	Category	Category Unique Identifier
IDENTIFY	ID	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
PROTECT	PR	Identity Management, Authentication and Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes and Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
DETECT	DE	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
RESPOND	RS	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
RECOVER	RC	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

461 Concurrent with the development of this LNG Profile, NIST published an initial public draft of
462 NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security [9]. The revision
463 includes additional alignment with other OT security standards and guidelines, including the
464 CSF. This initial draft of NIST SP 800-82 Rev. 3, Guide to (OT) Security has a section dedicated
465 to applying the CSF to OT in which all CSF Functions and selected CSF Categories and
466 Subcategories are covered. Readers may find it useful to reference it as a companion document
467 to this Profile.

3.2. Cybersecurity Framework Profiles

A Profile represents the outcomes based on business needs that an organization has selected from the CSF Categories and Subcategories. Profiles offer a prioritization of NIST CSF Categories and Subcategories based on the mission and operational considerations common to a specific group, such as the LNG sector with the MTS. Profiles serve as a useful starting point for identifying cybersecurity activities and outcomes that may be important to the selected group. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). They also offer an organization a consistent way to discuss cybersecurity objectives across organizational roles—from senior leadership to technical implementors—using common terminology. Individuals within the organization can use the Profile to prioritize the allocation of resources to cybersecurity improvements or to areas of particular concern.

Development of a Profile starts with the identification of an organization's mission objectives, high-level goals that must be achieved for the organization to succeed at its primary mission. The mission objectives provide the necessary context for an organization to manage its cybersecurity risk as it relates to a specific mission need. CSF Categories and Subcategories especially relevant to each mission objective are then identified and prioritized to fit the needs of the organization. Mission objectives identified in this CSF Profile are those that may be common to organizations in the LNG industry, but that individual mission objectives may vary by organization.

4. Cybersecurity Profile Development Methodology

Developing a Profile is a collaborative, stakeholder-driven process. To ensure that the Profile aligns cybersecurity outcomes with mission requirements, input from stakeholders and experts in a particular field is critical. This methodology lays out how NIST gathered input and garnered consensus from a group of LNG industry stakeholders to produce this Profile. This methodology is one approach to achieving consensus among stakeholders but is not the only way to do so.

4.1. Stakeholder Workshops

Profile workshops are conducted with stakeholders to establish agreed-on Mission objectives, prioritize those Mission objectives, and identify priority CSF Categories for each Mission objective. The output from these workshops serves as input for developing Profiles. The workshops are typically held in person, over the course of multiple days, with stakeholders and facilitators gathered in a single collaborative space. Workshops for this Profile occurred in the spring and summer months of 2021 during the COVID-19 pandemic. Facilitators conducted three separate online workshops with LNG industry stakeholders hereafter known as **participants**. Workshops were conducted under the assumption that participants could identify LNG assets critical to safety and emergency preparedness. The goals of these workshops were for the participants to:

- Identify and describe high-level Mission objectives for managing and maintaining LNG operations.
- Engage in a scoring exercise of the identified Mission objectives based on importance/criticality to LNG infrastructure.
- Engage in a prioritization exercise of the CSF Categories for each Mission objective.

509 Participants were from oil and natural gas corporations, infrastructure companies, U.S. LNG
510 export facilities, and individuals from other related LNG companies. The workshops are
511 described below.

4.1.1. Workshop 1: Establishing Mission Objectives

513 The first workshop [10] was conducted on May 13, 2021. In advance of the workshop,
514 participants were provided with an overview of the goals for the workshop and a copy of the
515 CSF.

516 During the workshop, facilitators provided an overview of the CSF and discussed why a CSF
517 profile is helpful as a construct for consistently managing cybersecurity risk. Facilitators then
518 shared a short example on how to create mission objectives. After working through the example,
519 facilitators guided participants through an activity focused on identifying candidate LNG
520 Mission objectives. The candidate mission objectives were designed to consider what business or
521 operational functions are critical to support LNG operations. After identifying an initial set of
522 candidate mission objectives, participants worked with each other and facilitators to refine a non-
523 prioritized list of consensus candidate mission objectives.

524 Following this session, participants received a non-prioritized list of consensus candidate mission
525 objectives and associated descriptions to prepare for workshop 2 and 3 discussions and exercises.

4.1.2. Workshop 2: Prioritizing Mission Objectives

527 The second workshop [11] was conducted on May 20, 2021. Facilitators led a mission objective
528 prioritization exercise known as the "Big Dog Scale" scoring system (used in previous CSF
529 development workshops) to identify the relative importance of each mission objective to LNG
530 operations. This scoring system entails participants assigning a score of 1, 3, 5, 8, or 13 to each
531 mission objective to indicate their importance within the overall mission of the LNG industry,
532 with 1 being the lowest, and 13 the highest. Experienced facilitators have found that the
533 asymmetry of this scale can help distinguish between scores (13 is intuitively more important
534 than 3, or even 8) and help facilitate discussion among participants.

535 Facilitators used their best judgment to select each mission objective such that lower importance
536 mission objectives would be scored earlier in the process. After assigning scores for the selected
537 mission objective, participants engaged in a facilitated discussion during which they explained
538 the reasoning behind each assigned score. The discussion offered opportunities for LNG industry
539 participants to offer some recommended actions for each mission objective. The recommended
540 actions are documented in Sec. 5 as "Organization should:" statements for each mission
541 objective. The CSF was not pushed by facilitators as a reference source for the language of the
542 recommended actions.

543 Once all candidate mission objectives were scored, the workshop ended with a brief review of
544 CSF Categories and the process as preparation for the next workshop on identifying high-priority
545 CSF Categories for inclusion in this Profile.

546 After the workshop, LNG industry participants' scores were analyzed to produce a prioritized
547 ranking of LNG mission objectives which appear in priority order in Table 2.

548   4.1.3. Workshop 3: Prioritizing CSF Categories for Mission Objectives

549   The final workshop [12] was conducted on May 27, 2021. Prior to this workshop, facilitators
550   distributed a scoresheet for participants to complete before the meeting. Participants were
551   instructed to identify the three most important CSF Categories for each mission objective,
552   assigning the Categories a score of 1 for the highest, then 2, then 3. For CSF Functions that did
553   not have any Categories scored as 1, 2, or 3, participants were asked to pick the Category for
554   each Function that best supports the mission objective. These categories were referred to as
555   "starred Categories."

556   During a facilitated discussion, participants shared the Categories they identified as important to
557   or supportive of each mission objective and explained how they arrived at their conclusions.
558   Participants provided input and adjusted their Category selections as discussions continued. For
559   each mission objective, participants' selections were recorded on a master scoresheet. At the end
560   of the workshop, the facilitators asked those whose scores had changed to send their updated
561   Category scoresheets to allow for updates to the master scoresheet.

562   Following the final workshop, participants' CSF Category selections were tallied to determine
563   relative priorities for Categories under each mission objective. This analysis is shown in Sec. 6.

564   4.2.   Subcategory Scoring

565   MITRE facilitated six Subcategory scoring sessions from June 9, 2021, to July 14, 2021, and
566   worked with participants to identify the relative importance of CSF Subcategories for each
567   Mission objective. During the scoring sessions, participants identified priorities for each CSF
568   Subcategory. For each Mission objective, facilitators walked the group through high-ranked
569   Categories. The group discussed and identified high- and medium-priority Subcategories, which
570   were marked with three dots and two dots, respectively. All other Subcategories in the section
571   were then noted with a single dot. Note that one Subcategory had additional considerations due
572   to the nature of the OT environment. Those Subcategories with additional consideration are
573   denoted using the "⊗" symbol in the dot charts in Sec. 7.

574   Next, the group ranked each of the three-dot, two-dot, and one-dot Subcategories by priority and
575   importance to distinguish between multiple Subcategories with the same dot allocation. This
576   process was repeated for medium-ranked categories, which were then starred. Some scoring
577   sessions had additional time remaining, which was used to revisit Categories that were not
578   indicated as high, medium, or starred during the Mission objectives weighted scoring workbook
579   analysis. These Categories underwent the same scoring and ranking process. Subcategory
580   priorities are shown in Sec. 7.

581   5. Marine Transportation System Liquefied Natural Gas Mission Objectives

582   Participants from the oil and natural gas industry participated in the online workshops and
583   identified nine Mission objectives for the LNG industry. Participants provided descriptions of
584   and summarized rationales for the ranked Mission objectives during workshop exercises and
585   discussions.

586   These Mission objectives were prioritized by the participants, and their prioritization is meant to
587   be informative rather than prescriptive. Each organization should consider its own goals and

588 priorities when consulting this Profile and adjust how the organization may apply guidance
589 accordingly.

590 **Table 2.** Liquefied Natural Gas Mission Objectives.

Priority	Mission Objective
1	Maintain Safe and Secure Operations
2	Ensure Operational Integrity of Plant Systems and Processes
3	Control Operational and Enterprise Security and Access
4	Monitor, Detect, and Respond to Anomalous Behavior
5	Safeguard the Environment
6	Define Policy and Governance Actions that Capture/Protect the Mission
7	Maintain Regulatory Compliance
8	Continuously Optimize and Maintain Current Operational State by Establishing Baselines and Measures
9	Validate and Optimize the Supply Chain

591 The LNG industry participants identified recommended actions for organizations to consider for
592 each mission objective. These recommended actions are shown as the bulleted text after
593 "Organizations should:" in the following sections.

594 ## 5.1. Mission Objective-1: Maintain Safe and Secure Operations

595 Organizations identify operational and cybersecurity vulnerabilities and threats that could affect
596 personnel safety and continuity of operations. Considerations include how to maintain regulatory
597 compliance and methods for securing the multi-operator environment. This Mission objective
598 results in the implementation of measures that prevent loss of plant control, infrastructure and
599 systems view, and proprietary information.

600 Organizations should:

601 • Manage risks to the organization and industry using a structured risk management
602 process.
603 • Ensure compliance with regulations put forth by governing bodies.
604 • Train personnel to be aware of proper usage of systems and equipment, process hazards,
605 and cybersecurity threats.
606 • Implement Detect/Respond/Recover activities where adverse events affect personnel
607 safety and security and incorporate lessons learned to enhance future security postures.

608 **Ranking Rationale:** Participants agreed that maintaining safe and secure operations is critical to
609 the LNG process. Safe and secure operations encompass activities such as establishing safety
610 procedures at the plant and among employees, training and education, and acknowledging safety
611 indicators. Human safety and the protection of human life are at the forefront of chief executive
612 officer-level discussions and are a critical part of maintaining plant security.

5.2. Mission Objective-2: Ensure Operational Integrity of Plant Systems and Processes

LNG operators look to ensure the integrity of hardware, software, and processes to prevent loss of control and continue operation of facilities. This includes the management of product and system lifecycles to guarantee sustained functionality and the verification of implemented processes for desired outcomes.

Organizations should:

- Employ administrative, physical, and technical safeguards on plant systems.
- Implement acquisitions management, change controls, and obsolescence and lifecycle management.
- Maintain product integrity through continuous quality testing, monitoring containment and shipments, and equipment inspection.
- Establish procedures for integrity measurement, including:
  - Systems testing
  - Preventive maintenance
  - Remediation
  - Ongoing situational awareness
  - Process review
- Architect fault-tolerant systems to maintain operational integrity during adverse events.
- Define policy to outline standard operating procedure to maintain repeatable processes with anticipated outcomes.

Ranking Rationale: The Mission objective captures the necessary measures for maintaining plant and equipment safety. Those activities (e.g., maintaining plant systems, preventing breaches) are crucial to ensuring operational integrity both in the plants and during the liquefaction process. For the LNG lifecycle to function safely and efficiently, implementations to support this Mission objective need to be present on the systems and operational sides.

5.3. Mission Objective-3: Control Operational and Enterprise Security and Access

LNG industry partners maintain their security profiles by identifying security risks and applying controls to mitigate them with a goal of preventing breaches that will impact operations. This can be achieved through understanding business workflow; event monitoring, detection, and logging; controlling physical and remote access to sites, systems, and assets; and revising current security policies based on ongoing risk-measurement processes and findings.

Organizations should:

- Establish separation between safety systems, distributed control systems, and other operational technology.
- Monitor network activity and inspect incoming data and payloads for threats to systems.
- Identify and train personnel on interdependencies between cybersecurity and operational responsibilities.
- Control physical and technical access to infrastructure and systems.

653   • Ensure confidentiality of sensitive data, plans, and procedures, with an emphasis on
654   sensitive data.

655 **Ranking Rationale:** This Mission objective emphasizes the importance of having safeguards in
656 place to protect the physical security and cybersecurity of LNG plants and ports, which includes
657 concerns with access. Participants noted that protection of OT is critical; therefore, processes and
658 procedures need to be in place to control access to the plants and systems (e.g., access to
659 workstations, vetting process, plant locations) as well as the information systems required to
660 manage the access control (e.g., badge readers, surveillance cameras). This Mission objective
661 was ranked in this order because it is imperative to the success of maintaining human and
662 equipment safety.

663 ## 5.4.   Mission Objective-4: Monitor, Detect, and Respond to Anomalous Behavior

664 LNG operations must include monitoring for anomalous activity to maintain situational
665 awareness. To detect anomalies, security baselining of the operation may be necessary. Detected
666 activity is correlated against other events in order to extrapolate indicators of compromise
667 supporting an organization's ability to disrupt the cyber kill-chain.

668 Organizations should:

669   • Monitor the behavior of personnel, machinery, and systems using methods that are robust
670   while also maintaining privacy.
671   • Detect anomalous behavior of personnel, machinery, and systems efficiently and
672   accurately.
673   • Respond to anomalous behavior of personnel, machinery, and systems using effective
674   and highly structured mechanisms.

675 **Ranking Rationale:** Participants stated that once a baseline is established to determine what
676 constitutes normal behavior of an LNG plant, it then becomes necessary to monitor for
677 deviations and possible events. Additionally, some participants viewed recovery and remediation
678 efforts as important actions in maintaining LNG operations.

679 ## 5.5.   Mission Objective-5: Safeguard the Environment

680 The integrity of the environment must be protected to maintain the sustainability of operations
681 and the organization's mission. Effects of malicious cyber activities on process control systems
682 can have a significant impact on the environment.

683 Organizations should:

684   • Identify cybersecurity risks that could impact the environment.
685   • Apply structured processes to manage risks to the environment.
686   • Train personnel that cybersecurity risk and environmental risk are interrelated.
687   • Manage the prominent and increasing roles of automated systems in maintaining quality
688   control of processes that may impact the environment.
689   • Implement Detect/Respond/Recover activities where cybersecurity incidents may result
690   in an adverse impact on the environment.
691   • Adhere to safety protocols.

692 **Ranking Rationale:** Participants reported that safeguarding environmental integrity is
693 significant for public safety and from a business perspective for the LNG industry.
694 Environmental incidents can cause irreparable damage to humans and ecosystems. Culpable
695 organizations face legal consequences, loss of brand reputation, and decreased profits. According
696 to participants, these incidents are often a byproduct of deficiencies in safety processes or
697 technologies in plant systems. Additionally, ensuring the physical security and cybersecurity of
698 plant systems can help to safeguard environmental integrity.

699 ## 5.6. Mission Objective-6: Define Policy and Governance Actions that
700 Capture/Protect the Mission

701 Policy and governance actions should include development of documented cybersecurity plans,
702 processes, and procedures.

703 Organizations should:

704 • Define business policy to encapsulate and promote a clear understanding of the mission
705   objectives, operations, and safeguards.
706 • Define governance actions that ensure the mission.

707 **Ranking Rationale:** This Mission objective covers business policy that governs the LNG
708 industry, including processes, vessels, technology, and physical sites. Individual organizational
709 policies not only pave the way toward complying with government regulations but will also
710 strengthen the organization's cybersecurity culture. Participants viewed governance as
711 foundational for both establishing best practices and making improvements in other areas of the
712 business. As such, governance should also be foundational for establishing best practices and
713 making improvements to cybersecurity risk mitigation. Additionally, it is important in driving
714 and supporting the goals and standards that the organization is trying to reach.

715 ## 5.7. Mission Objective-7: Maintain Regulatory Compliance

716 Organizations ensure operational plans and procedures are in accordance with regulatory
717 standards and best practices to maintain operations. Protocols and procedures are established and
718 aligned at the organizational level to facilitate regulatory compliance.

719 Organizations should:

720 • Maintain updated systems including IT/OT, and upgrade/patch systems as necessary.
721 • Ensure a safe and secure vessel and facility environment.
722 • Adhere to risk tolerance thresholds that meet regulatory standards.
723 • Develop and maintain plans and procedures that detail maintenance of devices and
724   process monitoring. The plans and procedures should reflect accepted levels of risk
725   outlined in organizational risk management procedures.
726 • Identify activities that can be completed to accomplish/meet the Mission objective.

727 **Ranking Rationale:** When ranking Mission objective 7, participants stated that maintaining
728 regulatory compliance is necessary to ensure safety for humans, the environment, and the plant.
729 Failure to comply with regulations can result in legal and financial ramifications and lead to

730 plant shutdowns. Compliance can act as a baseline with varying levels of maturity within
731 different areas. Mission objectives 6 and 7 share similarities; however, regulatory compliance
732 was ranked below corporate governance because participants stated that if governance is well
733 established and followed, then compliance will happen naturally.

734 **5.8.   Mission Objective-8: Continuously Optimize and Maintain Current**
735 **Operational State by Establishing Baselines and Measures**

736 Organizations operate iteratively to elevate "actual state" to "desired state" by clearly defining
737 events, threshold triggers, and remediation efforts in corporate policies.

738 Organizations should:

739 • Determine a schedule and develop a plan for efficacy measures, which include testing,
740   preventative maintenance, remediation, and ongoing situational awareness.
741 • Establish and leverage communication paths and trend data from devices to identify
742   deviations from baseline traffic flows.
743 • Document training and awareness procedures for potential cybersecurity risk vectors.

744 **Ranking Rationale:** This Mission objective entails establishing baselines in order to bring the
745 actual business state in line with the desired business state. These measurements are critical for
746 maintaining quality control but also for making improvements on equipment and processes.
747 Participants deemed that by following corporate governance and regulatory compliance
748 standards, which are both higher-ranked Mission objectives, quality control would be done by
749 default.

750 **5.9.   Mission Objective-9: Validate and Optimize the Supply Chain**

751 Organizations mitigate supply chain risks in the procurement of information and
752 communications technology and services through clear vendor agreements and established
753 processes and procedures (including testing) prior to installation and updates.

754 Organizations should:

755 • Vet vendors and suppliers when purchasing hardware, software, and system components
756   as well as when implementing configuration control.
757 • Ensure third-party vendor controls and cybersecurity maturity levels align with the
758   organization.
759 • Identify and streamline current business acquisition processes to optimize the
760   implementation of cybersecurity standards, protocols, and best practices across the
761   enterprise risk management plan.

762 **Ranking Rationale:** Participants maintained that handling the supply chain is important but
763 indicated that certain aspects were beyond the organization's control. They stated that a large
764 aspect of the supply chain is vetting other companies and third parties for best practices and a
765 cybersecurity maturity level that aligns with the organization's maturity level. Implementing
766 protections internally and establishing communication with vendors can help protect both the
767 business and its partners from unintended consequences.

6. Category Prioritization Summary

Workshop participants were asked to identify Categories most relevant to each Mission objective, and then to prioritize those Categories as high-priority, medium-priority, or starred-priority using the following descriptions:

- **High-Priority** Categories were considered the most critical for accomplishing a Mission objective.

- **Medium-Priority** Categories were considered important to a Mission objective, although not as important as high-priority Categories.

- **Starred-Priority** Categories were identified as being relevant to a Mission objective, but not with the same urgency as other priority Categories.

Profiles should be tailored to individual operating environments and organizational risk tolerances. The identified Category priorities, shown in Sec. 6.1, are intended to help focus resources on cybersecurity activities that participants identified as particularly relevant. The intent of this Profile is to suggest areas of priority focus pertinent to the LNG lifecycle. A user of this Profile could repeat the workshop steps to develop their own Profile based on their organization's unique needs and resource considerations.

The tables in Sec. 6.1 do not include the following Categories: Awareness and Training (PR.AT), Detection Processes (DE.DP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), Improvements (RS.IM), Improvements (RC.IM), and Communications (RC.CO). The workshop participants did not identify these Categories as relevant during the workshop. An organization should review all Categories when identifying high-priority, medium-priority, and starred-priority Categories on which it needs to focus.

6.1. Prioritized Cybersecurity Framework Categories by Mission Objective

Table 3. Prioritized CSF Categories for Mission Objective-1: Maintain Safe and Secure Operations.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY		Risk Assessment (ID.RA)	Asset Management (ID.AM)
PROTECT	Protective Technology (PR.PT)	Identity Management, Authentication and Access Control (PR.AC)	
DETECT		Security Continuous Monitoring (DE.CM)	
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

792
793

Table 4. Prioritized CSFs Categories for Mission Objective-2: Ensure Operational Integrity of Plant Systems and Processes.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Asset Management (ID.AM)	Risk Management (ID.RM)	
PROTECT		Maintenance (PR.MA) Protective Technology (PR.PT)	
DETECT			Security Continuous Monitoring (DE.CM)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

794
795

Table 5. Prioritized CSF Categories for Mission Objective-3: Control Operational and Enterprise Security and Access.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY			
PROTECT	Identity Management, Authentication and Access Control (PR.AC)	Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP)	
DETECT			Security Continuous Monitoring (DE.CM)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

796
797

Table 6. Prioritized CSF Categories for Mission Objective-4: Monitor, Detect, and Respond to Anomalous Behavior.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY		Asset Management (ID.AM)	
PROTECT			Information Protection Processes and Procedures (PR.IP)
DETECT	Anomalies and Events (DE.AE)		
RESPOND		Response Planning (RS.RP)	
RECOVER			Recovery Planning (RC.RP)

798   **Table 7.** Prioritized CSF Categories for Mission Objective-5: Safeguard the Environment.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Asset Management (ID.AM)	Governance (ID.GV)	
PROTECT	Data Security (PR.DS) Maintenance (PR.MA)		
DETECT			Anomalies and Events (DE.AE)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

799
800   **Table 8.** Prioritized CSF Categories for Mission Objective-6: Define Policy and Governance Actions that Capture/Protect the Mission.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Governance (ID.GV)	Business Environment (ID.BE)	
PROTECT		Information Protection Processes and Procedures (PR.IP)	
DETECT			Security Continuous Monitoring (DE.CM)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

801   **Table 9.** Prioritized CSF Categories for Mission Objective-7: Maintain Regulatory Compliance.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Governance (ID.GV)	Risk Assessment (ID.RA)	
PROTECT		Information Protection Processes and Procedures (PR.IP)	
DETECT		Anomalies and Events (DE.AE)	Security Continuous Monitoring (DE.CM)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

802
803   **Table 10.** Prioritized CSF Categories for Mission Objective-8: Continuously Optimize and Maintain Current Operational State by Establishing Baselines and Measures.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Asset Management (ID.AM)		
PROTECT		Data Security (PR.DS)	
DETECT	Security Continuous Monitoring (DE.CM)	Anomalies and Events (DE.AE)	
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

804   **Table 11.** Prioritized CSF Categories for Mission Objective-9: Validate and Optimize the Supply Chain.

Function	High Priority	Medium Priority	Starred Priority
IDENTIFY	Supply Chain Risk Management (ID.SC) Asset Management (ID.AM)		
PROTECT			Information Protection Processes and Procedures (PR.IP)
DETECT			Security Continuous Monitoring (DE.CM)
RESPOND			Response Planning (RS.RP)
RECOVER			Recovery Planning (RC.RP)

6.2. Summary Table

806 This table presents a summary of CSF Category relevance for all Mission objectives, to show
807 similarities and differences across Mission objectives.

808 In the tables, **H** stands for High Priority. **M** stands for Medium Priority. An asterisk (*) stands
809 for Starred Priority. These are categories that were prioritized for a Mission objective, but not
810 with the same urgency as other priority Categories.

811   **Table 12.** Summary Table of Mission Objectives with CSF Category Priorities.

	Mission Objectives								
	1	2	3	4	5	6	7	8	9
IDENTIFY									
Asset Management (ID.AM)	*	H		M	H			H	H
Business Environment (ID.BE)						M			
Governance (ID.GV)					M	H	H		
Risk Assessment (ID.RA)	M							M	
Risk Management Strategy (ID.RM)		M							
Supply Chain Risk Management (ID.SC)									H
PROTECT									
Access Control (PR.AC)	M		H		H				
Awareness and Training (PR.AT)									
Data Security (PR.DS)			M		H			M	
Information Protection Processes & Procedures (PR.IP)			M	*		M	M		*
Maintenance (PR.MA)		M			H				
Protective Technology (PR.PT)	H	M							
DETECT									
Anomalies and Events (DE.AE)				H	*		M	M	
Security Continuous Monitoring (DE.CM)	M	*	*			*	*	H	*
Detection Processes (DE.DP)									
RESPOND									
Response Planning (RS.RP)	*	*	*	M	*	*	*	*	*
Communications (RS.CO)									

	Mission Objectives								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Analysis (RS.AN)									
Mitigation (RS.MI)									
Improvements (RS.IM)									
RECOVER									
Recovery Planning (RC.RP)	*	*	*	*	*	*	*	*	*
Improvements (RC.IM)									
Communications (RC.CO)									

7. Priority Cybersecurity Framework Subcategories by Mission Objective

Following the workshops, the participants determined which CSF Subcategories were most relevant to each Mission objective.

7.1. Cybersecurity Framework Subcategory Priority Chart

Users of the Profile working to improve the security of the LNG industry should conduct activities in support of all applicable Subcategories of the CSF. This Profile recognizes and specifies a subset of those CSF Subcategories to help organizations prioritize cybersecurity risk mitigations they have yet to address. This Profile was developed to serve most of the LNG industry needs and, as such, was not developed to provide guidance on any action to be taken by an LNG organization. Those consulting this document should, as appropriate or necessary, emphasize (or de-emphasize) the importance of Subcategories depending on the unique needs of their organizations.

The "dot charts" in Tables 13–17 capture the relative importance of each CSF Subcategory to each Mission objective. From the perspective of the participants, who contributed to the development of this Profile, some CSF Subcategories are more critical than others to support the cybersecurity needs of LNG Operations Mission objectives. To that end, CSF Subcategories are divided into four types for the purposes of this Profile:

- **High Priority (●●●):** The most critical Subcategories for enabling a Mission objective in support of LNG operations. These Subcategories should be addressed most immediately given available resources.

- **Medium Priority (●●):** Subcategories that could be as urgent as high-priority Subcategories but most likely only in certain contexts or environments. Although considered lower priority, these Subcategories should be addressed to support the Mission objective; however, they may not need to be addressed as immediately as high-priority Subcategories.

- **Starred Priority (●):** Subcategories that are important to the overall cybersecurity of the Mission objective but may not require the same level of urgency as higher-priority Subcategories.

840   • **Additional Consideration (⊗):** Subcategories that require additional consideration due to
841   the unique properties and potential impacts to Operational Technology systems.

842   In this Profile, the Subcategory, **DE.CM-8: Vulnerability scans are performed**, is identified in
843   Table 15 as requiring additional considerations to highlight that vulnerability scans on OT
844   equipment may have a negative impact on achieving the following Mission objectives:

845   #2 - Ensure Operational Integrity of Plant Systems and Processes

846   #3- Control Operational and Enterprise Security and Access

847   #8- Continuously Optimize and Maintain Current Operational State by Establishing Baselines
848   and Measures

849   Concurrent with the development of this LNG Profile, NIST published an initial public draft of
850   NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security [9]. The revision
851   includes additional alignment with other OT security standards and guidelines, including the
852   CSF. This initial draft of NIST SP 800-82 Rev. 3, Guide to (OT) Security has a section dedicated
853   to applying the CSF to OT in which all CSF Functions and selected CSF Categories and
854   Subcategories are covered.

855   This initial draft of NIST SP 800-82 Rev. 3 highlights **OT-Specific Recommendations and**
856   **Guidance** for each Subcategory. Users may find the OT-Specific Recommendations and
857   Guidance for some Subcategories to be useful to identify additional considerations relevant to
858   their organization.

859   **Table 13.** CSF IDENTIFY (ID) Function Subcategory Priorities.

Function IDENTIFY	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
IDENTIFY (ID)	**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 organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	●●●	●●●	●	●●●	●●●	●	●	●●●	●●
		ID.AM-2: Software platforms and applications within the organization are inventoried	●●●	●●●	●	●●●	●●●	●	●	●●●	●●
		ID.AM-3: Organizational communication and data flows are mapped	●●●	●●●	●	●●●	●●●	●	●	●●	●●
		ID.AM-4: External information systems are catalogued	●●	●●●	●	●●●	●●●	●	●	●●●	●●●
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	●●●	●●●	●	●●	●●	●	●	●●	●●●
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●●	●●●	●	●●●	●●●	●	●	●	●
	Business Environment	**ID.BE-1:** The organization's role in the	●	●	●	●	●	●●●	●	●	●

Function IDENTIFY	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
	(ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	supply chain is identified and communicated									
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	●	●	●	●	●	●●●	●	●	●
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	●	●	●	●	●	●●●	●	●	●
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●	●	●	●	●	●●	●	●	●
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	●	●	●	●	●	●●	●	●	●
	Governance (ID.GV): The policies, procedures, and	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	●	●	●	●	●●●	●●●	●●●	●	●

Function IDENTIFY	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.		**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	●	●	●	●	●●	●●●	●●	●	●
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●	●	●	●	●●●	●●	●●●	●	●
		ID.GV-4: Governance and risk management processes address cybersecurity risks	●	●	●	●	●●●	●●●	●●●	●	●
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	●●●	●	●	●	●	●	●●	●	●
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	●●●	●	●	●	●	●	●	●	●
		ID.RA-3: Threats, both internal and external, are identified and documented	●●●	●	●	●	●	●	●	●	●
		ID.RA-4: Potential business impacts and likelihoods are identified	●●●	●	●	●	●	●	●●●	●	●
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●	●	●	●	●	●●●	●	●

Function IDENTIFY	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
		ID.RA-6: Risk responses are identified and prioritized	●●●	●	●	●	●	●	●●●	●	●
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	●●●	●●●	●	●	●	●	●	●	●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●●●	●●●	●	●	●	●	●	●	●
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●	●●●	●	●	●	●	●	●	●
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	●	●	●	●	●	●	●	●●●	●●●
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber	●	●	●	●	●	●	●	●●●	●●●

Function IDENTIFY	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
	managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	supply chain risk assessment process									
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	●	●	●	●	●	●	●	●	●●●
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	●	●	●	●	●	●	●	●	●●
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	●	●	●	●	●	●	●	●	●●●

860 **Table 14.** CSF PROTECT (PR) Function Subcategory Priorities.

Function PROTECT	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	●●●	●	●●●	●	●	●	●	●	●
		PR.AC-2: Physical access to assets is managed and protected	●●●	●	●●●	●	●	●	●	●	●
		PR.AC-3: Remote access is managed	●●●	●	●●●	●	●	●	●	●	●
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	●●●	●	●●	●	●	●	●	●	●
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	●●●	●	●●●	●	●	●	●	●	●
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	●●●	●	●●	●	●	●	●	●	●
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	●●●	●	●●	●	●	●	●	●	●

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
PROTECT			1	2	3	4	5	6	7	8	9
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	●●●	●	●	●	●	●●●	●	●	●
		PR.AT-2: Privileged users understand their roles and responsibilities	●●	●	●	●	●	●●●	●	●	●
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	●	●	●	●	●	●●	●	●	●
		PR.AT-4: Senior executives understand their roles and responsibilities	●	●	●	●	●	●●	●	●	●
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	●●	●	●	●	●	●●●	●	●	●
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality,	**PR.DS-1:** Data-at-rest is protected	●●●	●	●●●	●	●●●	●	●	●●	●
		PR.DS-2: Data-in-transit is protected	●●●	●	●●●	●	●●●	●	●	●●●	●
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●	●	●●	●	●●	●	●	●●	●
		PR.DS-4: Adequate capacity to ensure availability is maintained	●●●	●	●●●	●	●●●	●	●	●●●	●
		PR.DS-5: Protections against data leaks are implemented	●●	●	●●	●	●●●	●	●	●	●

Function PROTECT	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
	integrity, and availability of information.	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	●	●	●●	●	●●●	●	●	●●	●
		PR.DS-7: The development and testing environment(s) are separate from the production environment	●●	●	●●●	●	●●	●	●	●●●	●
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	●	●	●	●	●●●	●	●	●●	●
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	●●●	●	●●●	●●●	●	●●●	●●●	●	●●●
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	●●●	●	●●	●●	●	●●	●●●	●	●
		PR.IP-3: Configuration change control processes are in place	●●●	●	●●●	●●●	●	●●●	●●●	●	●●●
		PR.IP-4: Backups of information are conducted, maintained, and tested	●●	●	●●●	●●●	●	●●	●●	●	●●●
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	●	●	●●	●●●	●	●●●	●●●	●	●●

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
PROTECT	maintained and used to manage protection of information systems and assets.	**PR.IP-6:** Data is destroyed according to policy	●	●	●	●	●	●	●	●	●
		PR.IP-7: Protection processes are improved	●	●	●	●●	●	●●	●●	●	●●
		PR.IP-8: Effectiveness of protection technologies is shared	●	●	●	●	●	●●	●	●	●
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	●●	●	●●●	●●●	●●●	●●●	●●	●	●●●
		PR.IP-10: Response and recovery plans are tested	●●	●	●●●	●●●	●	●●	●●	●	●●
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	●●	●	●●●	●●	●	●●	●	●	●●
		PR.IP-12: A vulnerability management plan is developed and implemented	●●	●	●●	●●	●	●●	●	●	●●●
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	●●	●●●	●	●	●●●	●	●	●	●
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	●●	●●●	●	●	●●●	●	●	●	●

Function PROTECT	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	2	3	4	5	6	7	8	9
	performed consistent with policies and procedures.										
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	●●●	●●	●	●	●●	●	●	●	●
		PR.PT-2: Removable media is protected and its use restricted according to policy	●●	●●●	●	●	●	●	●	●	●
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	●●	●●●	●	●	●	●	●	●	●
		PR.PT-4: Communications and control networks are protected	●●●	●●●	●	●	●	●	●	●	●
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	●●●	●●●	●	●	●	●	●	●	●

861

Table 15. CSF DETECT (DE) Function Subcategory Priorities.

Function DETECT	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority, ⊗ = Additional Consideration								
			1	2	3	4	5	6	7	8	9
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	●●	●	●	●●●	●●●	●	●	●●●	●
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	●●	●	●	●●●	●●●	●	●	●●	●
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	●●●	●	●	●●●	●●●	●	●	●●●	●
		DE.AE-4: Impact of events is determined	●●	●	●	●●●	●●●	●	●	●●	●
		DE.AE-5: Incident alert thresholds are established	●	●	●	●●	●●	●	●	●●	●
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	●●●	●●●	●●●	●●●	●	●●	●●●	●●●	●●●
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●●●	●●●	●●●	●●	●	●●	●●●	●●●	●●
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	●●	●●●	●●●	●●●	●	●	●	●	●●●
		DE.CM-4: Malicious code is detected	●●●	●●●	●●●	●●●	●	●●	●●	●●●	●●●
		DE.CM-5: Unauthorized mobile code is detected	●●	●●	●●●	●●●	●	●	●●	●	●

33

Function DETECT	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority, ⊗ = Additional Consideration								
			1	2	3	4	5	6	7	8	9
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●●●	●●●	●●●	●●●	●	●●	●●	●●	●●●
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●●	●●●	●●●	●●●	●	●	●●	●●●	●●●
		DE.CM-8: Vulnerability scans are performed		⊗	⊗ ●●●	●●	●	●●	●	⊗	●●●
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	●●●	●	●	●	●	●	●	●	●
		DE.DP-2: Detection activities comply with all applicable requirements	●●●	●	●	●	●	●	●	●	●
		DE.DP-3: Detection processes are tested	●●●	●	●	●	●	●	●	●	●
		DE.DP-4: Event detection information is communicated	●●	●	●	●●	●	●	●	●	●
		DE.DP-5: Detection processes are continuously improved	●●	●	●	●●	●	●	●	●	●

862   **Table 16.** CSF RESPOND (RS) Function Subcategory Priorities.

Function RESPOND	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority								
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	●●●	●●●	●●●	●●●	●●	●●	●●●	●●	●●●
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	●●●	●●●	●	●●●	●●●	●	●	●	●
		RS.CO-2: Incidents are reported consistent with established criteria	●●●	●●	●	●●●	●●●	●	●	●	●
		RS.CO-3: Information is shared consistent with response plans	●●●	●●	●	●●●	●	●	●	●	●
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	●●	●●●	●	●●●	●●●	●	●	●	●
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader	●	●	●	●	●●●	●	●	●	●

| Function RESPOND | Category | Subcategory | Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority | | | | | | | | |
			1	2	3	4	5	6	7	8	9
		cybersecurity situational awareness									
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	●●●	●●●	●	●●●	●	●	●	●	●
		RS.AN-2: The impact of the incident is understood	●●●	●●●	●	●●	●	●	●	●	●
		RS.AN-3: Forensics are performed	●	●●●	●	●	●●●	●	●	●	●
		RS.AN-4: Incidents are categorized consistent with response plans	●	●	●	●	●	●	●	●	●
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)	●●	●●●	●	●●	●●●	●	●	●	●
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	●●●	●	●	●●●	●●●	●	●	●	●
		RS.MI-2: Incidents are mitigated	●●●	●	●	●●●	●●●	●	●	●	●
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●●	●	●	●●	●●	●	●	●	●

Function RESPOND			Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priority									
	Category	Subcategory	1	2	3	4	5	6	7	8	9
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	●●	●	●	●●	●	●	●	●	●
		RS.IM-2: Response strategies are updated	●●	●	●	●●	●	●	●	●	●

Table 17. CSF RECOVER (RC) Function Subcategory Priorities.

Function RECOVER			Mission Objectives ●●● = High Priority, ●● = Medium Priority, ● = Starred Priorities									
	Category	Subcategory	1	2	3	4	5	6	7	8	9
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	●●●	●●●	●●●	●●	●●●	●●	●●●	●●●	●●●

		of systems or assets affected by cybersecurity incidents.									
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	●●●	●	●	●●	●●●	●	●	●	●
		RC.IM-2: Recovery strategies are updated	●●●	●	●	●●	●●	●	●	●	●
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	●●	●	●	●	●	●	●	●	●
		RC.CO-2: Reputation is repaired after an incident	●●	●	●	●	●	●	●	●	●
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	●●	●	●	●●	●●	●	●	●	●

864

865 **7.2.   Subcategory Implementation Considerations**

866 This section consists of implementation considerations drawn directly from the discussions that
867 produced the Subcategory priorities provided in Tables 13-17. Implementation considerations
868 offer participant expertise and guidance about how a Subcategory fits LNG operational systems.

869 Concurrent with the development of this LNG Profile, NIST published an initial public draft of
870 NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security [9]. This initial draft of
871 NIST SP 800-82 Rev. 3 highlights **OT-Specific Recommendations and Guidance** for each
872 Subcategory. Users of this profile may find it useful to reference this OT focused draft to identify
873 additional implementation considerations.

874   **Table 18.** Implementation Considerations for Mission Objective-1: Maintain Safe and Secure Operations.

Function	Subcategory	Implementation Considerations
IDENTIFY	ID.AM-1,2,3	To manage risks to the organization, it must be understood what physical and software assets are present, what data exists on or is output from relevant systems, and who is involved in data handling and communications. In terms of priority, these controls are to be addressed sequentially.
PROTECT	PR.AC-7	Users may be required to authenticate, but most OT industrial control systems do not support multi-factor authentication (MFA) for all devices or assets. However, authentication is important to maintaining safe and secure LNG operations, so this control is high priority to push vendors and industry in the direction of supporting authentication measures (e.g., MFA, zero-trust architecture).
	PR.IP-3	Maintaining secure and tested backups is an essential part of maintaining the environment and ensuring its continued availability in case of data loss or system disruption. In achieving this Mission objective, organizations should consider ensuring control of what, when, and how something has changed within their environment.
DETECT	DE.CM-1,2,4,6,7	To achieve continuous monitoring, LNG facilities will need data regarding their network, physical environment, malware, etc. Many of these systems may currently have external vendors monitoring or collecting log data. Therefore, unauthorized activity, personnel, devices, and software will need to be monitored. It is recommended that detection capabilities exist at both the network and physical levels.
	DE.CM-8	Vulnerability scanning of OT systems requires special consideration. Traditional IT scanning methods could potentially disrupt the operation of an OT component. There are additional vulnerability identification methods for OT equipment that can be employed such as review of vendor or manufacturer updates.
RESPOND	RS.RP-1	Response plans may incorporate scenarios that could be hazardous for responders and incorporate appropriate human safety precautions to address those potential events. The effectiveness of response plans may be improved through training and tested through exercises of the plans.
RECOVER	RC.IM-1	Adverse events in the LNG industry may have significant impacts to the environment, economic security, and human safety. Holding lessons learned sessions following an adverse event can help an organization identify and control the causal factors of adverse events and improve response actions if such an event occurs.

Function	Subcategory	Implementation Considerations
	RC.CO-3	Effectively responding to an adverse event requires coordination across multiple organizational functions (e.g., engineering, operations, legal, and public relations) and potentially external stakeholders (e.g., government agencies, law enforcement, response vendors, and insurers).

Table 19. Considerations for Mission Objective-2: Ensure Operational Integrity of Plant Systems and Processes.

Function	Subcategory	Considerations
IDENTIFY	ID.AM-5	Prioritizing resources based on classification, criticality, and business value is crucial to executive-level risk management decisions, such as where to allocate funding to remediate security gaps. This subcategory also aligns with ISA/IEC 62443 guidelines of organizing your systems by priority and impact for assessment.
	ID.AM-6	Operators often do not have direct physical access to components deployed at LNG facilities due to the remote location of the components. Therefore, they often connect to these systems remotely. Remote access is a common threat vector for cyber-attacks and therefore it's important to carefully control remote access and stipulate how any third-party remote access would be managed, configured, and secured. The LNG industry relies heavily on partners for remote monitoring and diagnostics. There are explicit cybersecurity requirements built into some equipment agreements that stem from industry memorandums of agreements that need to be taken into account for access management.
PROTECT	PR.IP-1	Change control processes help to reduce the probability that changes to assets will cause an adverse operational event. Additionally, requirements for safe and efficient operations may be met by implementing configuration baselines that align with operational integrity requirements and a process to manage the configuration and deployment of assets.
DETECT	DE.CM-8	Vulnerability scans should not be run in an operational OT environment (unless their impact is fully understood), although passive scans or scans on backups may be feasible. For IT infrastructure, this subcategory may be required for threat management and continuous monitoring.
RESPOND	RS.AN-4	Development of thresholds for categorization of adverse events will be influenced by the unique operational needs of LNG processes and require input from a diverse set of stakeholders from across the organization, including operations, legal, and compliance team members.
RECOVER	RS.CO-1	Ensuring operational integrity of plant systems and process following a cybersecurity incident may necessitate operational shutdowns and a longer recovery for LNG systems. Communication may help to alleviate public concern that shutdowns were caused by threat actors and not by normal safety precautions during recovery.

Table 20. Considerations for Mission Objective-3: Control Operational and Enterprise Security and Access.

Function	Subcategory	Considerations
IDENTIFY	ID.AM-3	LNG operations and supporting business functions may, over time, develop interdependencies across IT and OT systems. Mapping the communication and data flows of IT and OT processes can help to identify interdependent

Function	Subcategory	Considerations
		systems by highlighting systems whose day-to-day operations require communications across systems.
PROTECT	PR.AC-6	In LNG operation control rooms, there are multiple operators that are documented in shift logs for visibility. Those identities should be proofed and bound. However, it is difficult to establish individual accountability when dealing with OT due to the presence of legacy systems. LNG security subject matter experts noted that access control improvements will be more prevalent in the future with the integration of zero-trust architecture to proof credentials. Currently, vendors may not allow that into their platforms. It is important that manufacturers improve those security practices. Two-factor authentication may be a good option to address this control.
	PR.DS-6	Integrity checking mechanisms may be built into IT and OT systems. Verification activities may include procedure or technical verification of software, firmware, hardware, etc. It's a medium priority because one is unable to conduct integrity checks on an active or running system; however, it is important to commit to integrity checking prior to commissioning a new system. Many safety systems for LNG have integrity checking for safety systems and basic process control systems.
	PR.IP-10,11	Cybersecurity should be included in human resources practices such as personnel screening and deprovisioning. Participants noted that there may be limitations on the types of personnel screening an organization can conduct. Personnel screening improvements should be improved by the LNG industry.
DETECT	DE.CM-8	Scans should be conducted when OT equipment is first acquired and during planned downtimes. Vulnerability scanning of OT systems requires special consideration since traditional IT scanning methods could potentially disrupt the operation of an OT component. There are additional vulnerability identification methods for OT equipment that can be employed such as review of vendor or manufacturer updates and USG vulnerability reporting.
RESPOND	RS.AN-1	Physical and logical access systems may generate a high volume of alerts that require investigation. Alerts related to critical assets may be prioritized above those related to non-critical assets to improve response times for assets that are most impactful to the organization.
RECOVER	RC.RP-1	Recovery may require access to be granted to third parties that would not have access outside of an adverse event. These may include law enforcement, vendors, government agencies, or peer organizations supporting recovery efforts. It may help to expedite these activities if access is provisioned in advance.

879   **Table 21.** Considerations for Mission Objective-4: Monitor, Detect, and Respond to Anomalous Behavior.

Function	Subcategory	Considerations
IDENTIFY	ID.AM-1,2,3,4	Regarding priority, these subcategories should be addressed in a sequential manner. An organization must have an inventory of its assets (physical devices, systems, and software). After developing an asset inventory, organizations will be able to map how inventoried assets communicate.
PROTECT	PR.IP-1	Implementation of asset configuration baselines and strong change management may help to support detection of changes to asset configurations.
DETECT	DE.AE-5	Development of baselines based on normal activity across the operating environment is critical for anomaly detection. Organizations may also consider developing incident declaration thresholds based on an

Function	Subcategory	Considerations
		understanding of normal activity and abnormal behavior that could cause operational disruptions.
RESPOND	RS.MI-1,2	Mitigating incidents is a high priority for LNG operations. However, if there is evidence of anomalous activities, it's important that the organization be able to contain the incident.
	RS.MI-3	Accepting risks is a medium priority, because an organization may only be able to address high-priority vulnerabilities due to the nature of OT. Organizations may not be able to roll out a patch, update, or fix known issues until the next shutdown or maintenance window.
RECOVER	RC.CO-3	Effective communications are important in the response to anomalous behavior. In LNG operations, there may be multiple business units and similar systems, regardless of whether they operate differently. There are often external stakeholders from the pipelines that require PLC-to-PLC communication or raw materials which may be sourced from different organizations. These pipeline and LNG partners should receive alerts when anomalous events are detected.

880   **Table 22.** Considerations for Mission Objective-5: Safeguard the Environment.

Function	Subcategories	Considerations
IDENTIFY	ID.GV-3	Internal policy should reflect regulatory requirements to ensure that environmental protections are in place.
PROTECT	PR.DS-1,2,4,5	Organizations should implement controls that meet defined confidentiality, integrity, and availability requirements.
	PR.MA-2	The industry is experiencing an increase in remote access utilization; for example, field service engineers remotely accessing platforms. Thus, controls and authorization processes need to be implemented to protect systems if those controls are not already in place.
DETECT	DE.AE-3	A common dilemma for LNG facilities is a lack of sensors deployed to extract data for security logs. This situation could be improved with a larger variety of data sources to gain insight into correlated cyber events.
	DE.AE-4	Identifying attack vectors and determining impact is important in order to put the correct protections in place and prioritize incoming alerts.
RESPOND	RS.AN-5	Many systems do not have an automated mechanism to identify vulnerabilities, so these systems require manual review of vendor vulnerability notifications. This vulnerability identification process must be robust whether manual or automated, because without it, organizations may overlook opportunities to mitigate known vulnerabilities.
RECOVER	RC.CO-1,2,3	In a mixed architecture environment, when environmental incidents occur, timely communication is important so that both the industry and its partners can quickly implement mitigation and recovery actions. Without effective communication, the organization may be potentially liable for inaction.
	RC.RP-1	The timeliness of recovery requires a readily executable plan. The longer it takes to recover from an incident, the higher the potential impact for the environment and the organization.

881
882

Table 23. Considerations for Mission Objective-6: Define Policy and Governance Actions that Capture/Protect the Mission.

Function	Subcategories	Considerations
IDENTIFY	ID.GV-1	Establishing policies for cybersecurity-related activities that align with organizational goals and objectives will help ensure that these activities fulfill the organization's mission, and they align with the organization's most-valued behaviors. Policies also enable organizations to assign responsibility for cybersecurity activities to specific roles and build procedures that help the organization to meet legal and regulatory requirements.
PROTECT	PR.AT-1	All users (e.g., IT traditional roles and users, operators) should be informed and trained in cybersecurity risks and measures related to LNG operations and technology.
	PR.IP-8	Internal sharing can be used to revise processes and reduce cost and risk as improvements are made.
DETECT	DE.CM-1,8	In both the IT and OT environments, scanning of systems and networks should be defined by policy including caveats based on feasibility. With these policies in place, employees can refer to them and know what actions to take for each system.
RESPOND	RS.CO-3,4	It may be necessary to notify external parties upon declaration of an incident to comply with legal or regulatory requirements. Incident response plans should document the stakeholders that must be notified, information that must be shared, and roles responsible for communications.
RECOVER	RC.RP-1	An incident may cause operational disruption, but recovery plans will help ensure that an organization can still meet its mission. Advanced planning and development of recovery plans will identify the resources necessary for reconstitution, describe activities necessary for restoring operations, and assign responsibility for key roles.

883

Table 24. Considerations for Mission Objective-7: Maintain Regulatory Compliance.

Function	Subcategories	Considerations
IDENTIFY	ID.RA-3	Examples of threats for consideration: script kiddies, dedicated hackers, nation-states, cyber-criminals, insider threats (both malicious and accidental).
	ID.RA-4	Traditionally, likelihood has been easier to measure in spaces that provide concrete numeric data, such as equipment failure rates. Likelihood for cybersecurity risks can be more difficult to estimate.
PROTECT	PR.AT-1	Cybersecurity awareness activities can be used to notify employees of regulatory compliance requirements, communicate expected behavior, and improve employee understanding of cyber risks.
DETECT	DE.CM-1,2,4,5	These controls are high and medium priority due to the regulations in place for the physical environment or facility of LNG operations. There may be third parties, that have remote access to the technology, so network monitoring is a priority. There has been increasing tablet presence and cellphone connectivity to industrial control systems in general as well as within the LNG sector. Additionally, there may be cell modem connectivity into regulatory systems. Hence, the two-dot consideration for DE.CM-5.
	DE.CM-8	Certain older devices may not support vulnerability scanning due to the inherent limitations of the technology.
RESPOND	RS.CO-2,3	Incident response plans should be developed to help organizations meet regulatory requirements, including deadlines for reporting an incident, stakeholders that must receive notification, and reporting requirements.

Function	Subcategories	Considerations
RECOVER	RS.CO-3	Similar to incident reporting, necessary regulatory reporting related to recovery activities should be built into response plans.

884
885
Table 25. Considerations for Mission Objective-8: Continuously Optimize and Maintain Current Operational State by Establishing Baselines and Measures.

Function	Subcategories	Considerations
IDENTIFY	ID.SC-1	Suppliers and third parties can introduce risk that might reduce an organization's ability to maintain a desired operational state. Cyber supply chain risk management processes may be integrated with an enterprise-level risk management program or may be operated separately but provide inputs to an enterprise-level risk management program.
PROTECT	PR.DS-4	Development of plans to elevate the organization's actual state to a desired state should consider additional resources that might be necessary to achieve business goals and maintain availability of operational processes.
DETECT	DE.AE-3	Collecting data from multiple sources in an environment and for a variety of events helps to establish the baseline for what is occurring in the environment. These baselines can then be used to distinguish attacks or incidents from false positives.
	DE.CM-2	Certain types of equipment cannot reliably be detected through the network, or they require manual discovery, monitoring, and control. In cases where cybersecurity controls are not feasible, a physical access control may be applied as a mitigating measure to protect operational equipment.
	DE.CM-5	In the future, if the ability to connect wirelessly to sensors continues to grow, this subcategory will become an increasingly significant concern to the OT cybersecurity professionals tasked with maintaining the secure operation of these systems.
	DE.CM-8	Direct scanning should not be done on an operational network given the potential for disruption of an Industrial Control System (ICS) or OT environment. Frequent scans on the legacy equipment could lead to failure of the PLCs and other ICS devices on an operational network. Vulnerability scans against backups or offline systems could be conducted to mitigate those risks.
RESPOND	RS.RP-1	Implementation of additional capabilities to reach a desired state should also drive updates to incident response plans to ensure they still align with production equipment and processes.
RECOVER	RC.RP-1	As organizations progress to a desired state, updates to recovery plans may be necessary as new capabilities may require additional consideration for restoration activities.

886
Table 26. Considerations for Mission Objective-9: Validate and Optimize Supply Chain.

Function	Subcategories	Considerations
IDENTIFY	ID.AM-1,2	From an IT perspective, ID.AM-2 may have a higher priority than ID.AM-1. This is due to having more external-facing systems, like enterprise scheduling, billing, or tolling applications that are important from a supply chain standpoint. From an OT perspective, ID.AM-1 is a higher priority because there are more systems that can only be internally and physically accessed. Cataloging the software platforms and applications is often a byproduct of inventorying the physical equipment.

Function	Subcategories	Considerations
	ID.AM-4	Organizations may have functions that are supported by third parties, such as alternative facility power sources. These external systems can have direct connections into site systems, which puts them at risk for attack if the third party is compromised. It is important to understand which systems have external connections so that they can be monitored.
	ID.SC-3	Contracts with suppliers and third parties provide legal protections in case of an incident. Many companies rely on the third party's ability to deliver cyber controls and cybersecurity capabilities within the context of that contract. A weak contract puts companies at risk from reputational, legal, and financial perspectives.
PROTECT	PR.IP-2	In the OT environment, it may be more difficult to manage the software development lifecycle, as it is largely controlled by the vendor.
	PR.IP-12	From a supply chain perspective, vulnerability management should include managing software updates and bug fixes that come from vendors.
DETECT	DE.CM-8	Vulnerability scanning and endpoint detection may require an agent to first be implemented in the equipment or technology. Adding an agent could void the vendor warranty, and an organization may value keeping the warranty over the benefits of setting up scanning for some of its OT components.
RESPOND	RS.RP-1	Incident response plans should include scenarios related to incidents that stem from supply chain vulnerabilities, such as an application that introduces a vulnerability into the operational environment or a service provider that suffers from a breach.
RECOVER	RC.RP-1	Recovery activities that may require coordination with third parties should be documented in recovery plans, as well as contractual agreements with third parties.

References

[1] National Institute of Standards and Technology (2018), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2] U.S. Energy Information Administration EIA (2022) *US Energy Facts Explained.* Available at: https://www.eia.gov/energyexplained/us-energy-facts/

[3] U.S. Department of Energy. *Liquefied Natural Gas (LNG).* Available at: https://www.energy.gov/fe/science-innovation/oil-gas/liquefied-natural-gas

[4] U.S. Department of Energy (2013) *Liquefied Natural Gas: Understanding the Basic Facts.*

[5] Title 33 Chapter I Subchapter P Part 165 Subpart D § 165.33 -- maritime security: Facilities (2022). Available at: https://www.ecfr.gov/current/title-33/chapter-I/subchapter-P/part-165/subpart-D/section-165.33

[6] U.S. Department of Homeland Security (2013) National Infrastructure Protection Plan. Available at: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[7] U.S. Committee on the Marine Transportation System (n.d.) *Why the MTS Matters*, Available: https://www.cmts.gov/why-cmts-matters/

[8] Mahn A, Marron J, Quinn S, Topper D (2021) Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1271. Available at: https://doi.org/10.6028/NIST.SP.1271

[9] Stouffer K, Pease M, Tang C, Zimmerman T, Pillitteri V, Lightman, S (2022) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 3. Available at: https://doi.org/10.6028/NIST.SP.800-82r3.ipd

[10] Long J, Thompson M, Ayala M, Beebe T, Belisle M, Girdner A, Casey C, Collins C, Tran H, Herriott A, Yates C, Newhouse B, El-Najjar K, Wynn D, Northrip D, Davis P, Shires D, Weitzel D, Fitzpatrick D, Wallace C, Savoury R, Mann D, DeMoura D (2021) Marine Transportation Systems LNG Cybersecurity Industry Profile Online Workshop 1, The MITRE Corporation, May 13, 2021 (10:00 a.m. to 12:30 p.m. EDT).

[11] Long J, Thompson M, Ayala M, Beebe T, Casey C, Collins C, Tran H, Herriott A, Newhouse B, Wynn J, Northrip D, Weitzel D, Fitzpatrick D, Savoury R, Mann D, Alvarado O, Brule J, Pace K, Byrne T, Bloom C, Yates C, Davis P, Yamben W, Philibert R, El-Najjar K, DeMoura D (2021) Marine Transportation Systems LNG Cybersecurity Industry Profile Online Workshop 2, The MITRE Corporation, May 20, 2021 (10:00 a.m. to 12:30 p.m. EDT).

[12] Long J, Thompson M, Ayala M, Beebe T, Casey C, Collins C, Tran H, Herriott A, Newhouse B, Wynn J, Northrip D, Shires D, Weitzel D, Fitzpatrick D, Wallace C, Savoury R, Mann D, Alvarado O, Brule J, Pace K, Mouton J, Muneer F (2021), Marine Transportation Systems LNG Cybersecurity Industry Profile Online Workshop 3, The MITRE Corporation, May 27, 2021 (10:00 a.m. to 12:30 p.m. EDT).

[13] National Institute of Standards and Technology, Glossary, Available at: https://csrc.nist.gov/glossary

930 ## Appendix A. List of Symbols, Abbreviations, and Acronyms

931 Selected acronyms and abbreviations used in this document are defined below.

932 **BOG**
933 Boil-Off Gas

934 **CESER**
935 Office of Cybersecurity, Energy Security, and Emergency Response

936 **CSF**
937 Cybersecurity Framework

938 **ICS**
939 Industrial Control Systems

940 **IT**
941 Information Technology

942 **JT**
943 Joule-Thomson

944 **LNG**
945 Liquefied Natural Gas

946 **MFA**
947 Multi-Factor Authentication

948 **MTS**
949 Marine Transportation System

950 **NCCoE**
951 National Cybersecurity Center of Excellence

952 **NIST**
953 National Institute of Standards and Technology

954 **OT**
955 Operational Technology

956 **PLC**
957 Programmable Logic Controller

958 **Appendix B. Glossary**

959 Source: NIST Computer Security Resource Center Glossary [13]

960 **Category**
961 The subdivision of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and
962 particular activities.

963 **Framework**
964 The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common
965 language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes
966 activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those
967 outcomes.

968 **Function**
969 Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

970 **Mission Objective**
971 A high-level goal that must be achieved for an organization to succeed at its primary mission or purpose.

972 **Profile**
973 A representation of the outcomes that a particular system or organization has selected from the CSF Categories and
974 Subcategories.

975 **Subcategory**
976 The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of
977 Subcategories include "External information systems are cataloged," "Data-at-rest is protected," and "Notifications
978 from detection systems are investigated."