# Pipeline Cybersecurity

API STANDARD 1164

THIRD EDITION, Mmm 202y

American
Petroleum
Institute

This Page is Intentionally Left Blank

## Foreword

This standard provides requirements and guidance for the owner/operators of oil and natural gas industry for managing cyber-risk associated with their industrial automation control (IAC) environments to achieve integrity and security objectives. The scope of this document is focused on, but not limited to, pipelines regulated under *Title 49 CFR Part 192 – Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards or Title 49 CFR Part 195 - Transportation of Hazardous Liquids by Pipeline*, but should be used in the context of developing and implementing security policies, processes, procedural and technical security controls for their IAC Cyber Environments, include SCADA, local control, and IIoT solutions. This document embodies the API's *Security Guidelines for the Petroleum Industry*.

This standard is specifically written to provide the operators with industry targeted IAC cybersecurity requirements and practices, and the framework needed to develop a robust IAC security program as part of the U.S. Transportation Security Administration required Corporate Security Program.

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

## API Standards Process

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 200 Massachusetts Ave, NW, Washington, DC 20001. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 200 Massachusetts Ave, NW, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Ave, NW, Washington, DC 20001, standards@api.org.

This Page is Intentionally Left Blank

# TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

# 1 Scope

## 1.1 Purpose

This Standard was developed to provide an actionable approach to manage cybersecurity risk and protect the essential functions of industrial automation and control environments. It is tailored for the oil and natural gas (ONG) pipeline industry. This includes, but is not limited to, natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, liquefied natural gas facilities, propane air facilities, and others involved in these industries. It is a set of requirements to help manage the cybersecurity posture and any resulting residual risk to industrial control environments in alignment with the operator's mission, objectives, risk strategy, and in accordance with its policies and procedures.

This Standard was developed using the US National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.1, April 16, 2018* (CSF), addressing all Functions, Categories and Subcategories. Activities were selected from the Framework Core with a focus and scoping of industrial automation control systems. Special attention was given to common risk management considerations (e.g. an institutionalized health and safety culture, environmental protection priorities, participation in critical infrastructure, providing critical products and services, etc.), legal/regulatory requirements (e.g. TSA, FERC, DOT PHMSA, etc.), and shared business/mission objectives (e.g. Protecting reputation with all stakeholders and positive public opinion).

This Standard focuses on desired cybersecurity outcomes and is, in effect, a "Target Profile". A "Current Profile" is represented by the outcomes of the CSF Core that are currently implemented and being achieved in its industrial automation and control environments. This Target Profile and the Current Profile can be compared identifying opportunities for improving the current cybersecurity posture and influencing process improvement priorities of the pipeline systems. Refer to NIST CSF for definitions of Target Profile and Current Profile.

Prioritizing the mitigation of the gap between current and target profiles is driven by the organization's business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner. The following are examples of how the Target Profile may be used:

- An operator shall use it as its industrial cybersecurity program baseline.
- An ONG pipeline industry member may extend it to build a more risk-based tailored industrial cybersecurity program.
- An ONG pipeline industry member may utilize the Target Profile to express industrial cybersecurity risk management requirements to an external service provider.
- An ONG pipeline industry member may express a system's cybersecurity state through a Current Profile to report results relative to the Target Profile.
- An ONG pipeline industry member, having identified an external partner upon whom its infrastructure depends, may use the Target Profile to convey required cybersecurity outcomes.

## 1.2 Intended Audience

This document covers details specific to pipeline systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Senior management trying to understand implications and consequences as they justify and implement a pipeline system's cybersecurity program to mitigate business functionality impact.
- Managers who are responsible for pipeline systems.
- System administrators, engineers, and information technology (IT) professionals who administer, patch, or secure pipeline systems.
- Control engineers, integrators, and architects who design or implement secure pipeline systems.
- Software manufacturers.
- Products and services vendors.

- Regulators responsible for pipeline cyber security.
- Other government stakeholders trying to understand the unique pipeline security needs.
- Researchers, academic institutions, and analysts who are trying to understand the unique security needs of pipeline systems.

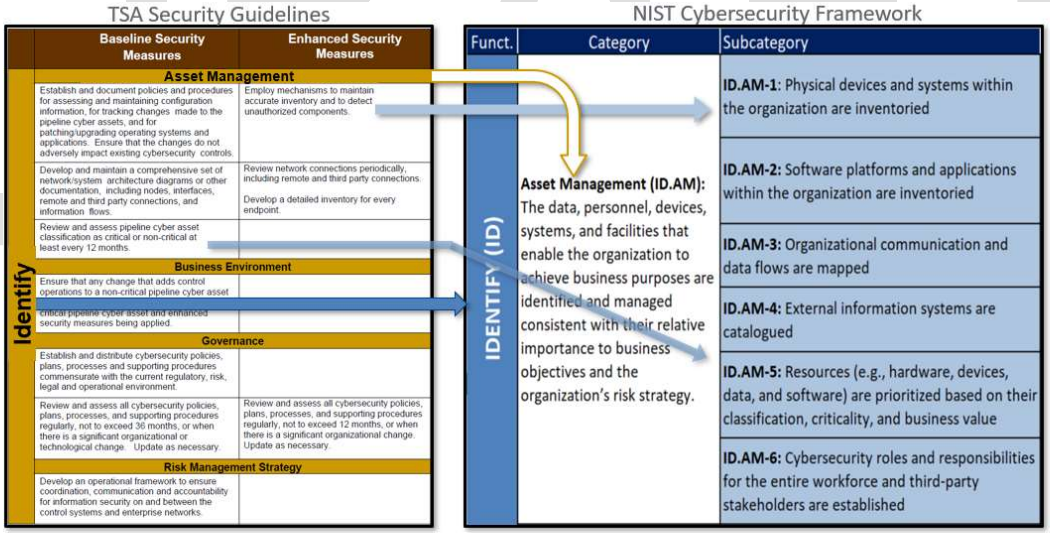
## 1.3 How to Read This Standard

In the context of this document, the terms industrial automation control system(s), industrial control system(s), or control system(s) refers to Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS) and local control systems used in the oil and natural gas industries. It does not refer to Safety Instrumented Systems (SIS), unless explicitly called out, as those are out of scope of this document. When the term SCADA or DCS is used it refers to SCADA or DCS systems only and not local control systems. The converse is also true; when the term local control system is used it is distinguishing the system from a SCADA or DCS system with which it may interact.

### 1.3.1 US TSA Pipeline Security Guidelines Inclusion

The US Transportation Security Administration (TSA) maintains a Pipeline Security Guidelines document. The scope of TSA's guidelines is applicable to operational natural gas and hazardous liquid transmission pipelines, natural gas distribution pipeline systems, and liquified natural gas facility operators. They are also applicable to operational pipeline systems that transport materials categorized as toxic inhalation hazards. The TSA guidelines provide criteria which operators must use to assess and determine criticality of each of their facilities. In addition, the guidelines identify baseline security risk reduction measures that must be implemented at each facility, as well as enhanced measures that must be implemented at facilities determined to be critical.

In March of 2018, TSA issued a revised version to address challenges in the everchanging security landscape. A significant update implemented was to align the TSA cybersecurity principles, aspects, and requirements to the NIST CSF. They did this by mapping their Baseline and Enhanced Security Measures to the NIST Framework Core.



TSA Security Guidelines

| | Baseline Security Measures | Enhanced Security Measures |
|---|---|---|
| Identify | **Asset Management** | |
| | Establish and document policies and procedures for assessing and maintaining configuration information, for tracking changes made to the pipeline cyber assets, and for patching/upgrading operating systems and applications. Ensure that the changes do not adversely impact existing cybersecurity controls. | Employ mechanisms to maintain accurate inventory and to detect unauthorized components. |
| | Develop and maintain a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third party connections, and information flows. | Review network connections periodically, including remote and third party connections.<br>Develop a detailed inventory for every endpoint. |
| | Review and assess pipeline cyber asset classification as critical or non-critical at least every 12 months. | |
| | **Business Environment** | |
| | Ensure that any change that adds control operations to a non-critical pipeline cyber asset critical pipeline cyber asset and enhanced security measures being applied. | |
| | **Governance** | |
| | Establish and distribute cybersecurity policies, plans, processes and supporting procedures commensurate with the current regulatory, risk, legal and operational environment. | |
| | Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 36 months, or when there is a significant organizational or technological change. Update as necessary. | Review and assess all cybersecurity policies, plans, processes, and supporting procedures regularly, not to exceed 12 months, or when there is a significant organizational change. Update as necessary. |
| | **Risk Management Strategy** | |
| | Develop an operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks. | |

NIST Cybersecurity Framework

| Funct. | Category | Subcategory |
|---|---|---|
| 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 business 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, 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 are established |

**Figure 1-1: TSA Cybersecurity Measures to CSF Core Mapping**

The Baseline Measures and Enhanced measures specified in TSA Pipeline Security guidelines are used to apply a security control rating of Baseline or Enhanced. API 1164 has leveraged this and refined it into three levels of security protections.

### 1.3.2 NIST Cyber Security Framework Foundation

The NIST Cyber Security Framework allows significant freedom in how it its used or implemented. This is reinforced by clearly stating that the presentation format chosen for the Framework Core is not to be interpreted as prescribing a security programs implementation order or priority. This standard leverages this flexibility to align the Framework Core to one of its guiding tenets: actionable and thereby implementable.

This tenet is manifested by way of reordering the CSF Subcategories within a CSF Category in this Standard to follow a foundational-elements → primary-elements → secondary-elements approach. This is especially true in the

Identity (ID) Function. The subcategories of the Governance Category, and especially the activities of the ID.GV-1 – IAC Cybersecurity Plan subcategory, are foundational to a security program. That is, an organizationally approved Industrial Cybersecurity Policy is the cornerstone and authorization for all other cybersecurity components and activities. The Policy must mandate an Industrial Cybersecurity Program be implemented and that it is defined by a formal plan. The Industrial Cybersecurity Plan specifies all requirements and outcomes of the Industrial Cybersecurity Program. These are all foundational building elements of a sound security posture that can be matured and risk-appropriately strengthened over time.

Another foundational element is the ability to strengthen the security posture in appropriate ways, at the appropriate time, and in the appropriate places. This is accomplished by developing an organizationally appropriate risk management strategy. This guides the implementation of a Risk Management Program, which includes a risk assessment process to prioritize resources for the areas in most need (highest risk).

This results in the Framework's Core being realigned to the API 1164 order as depicted in Figure 1-1 below.

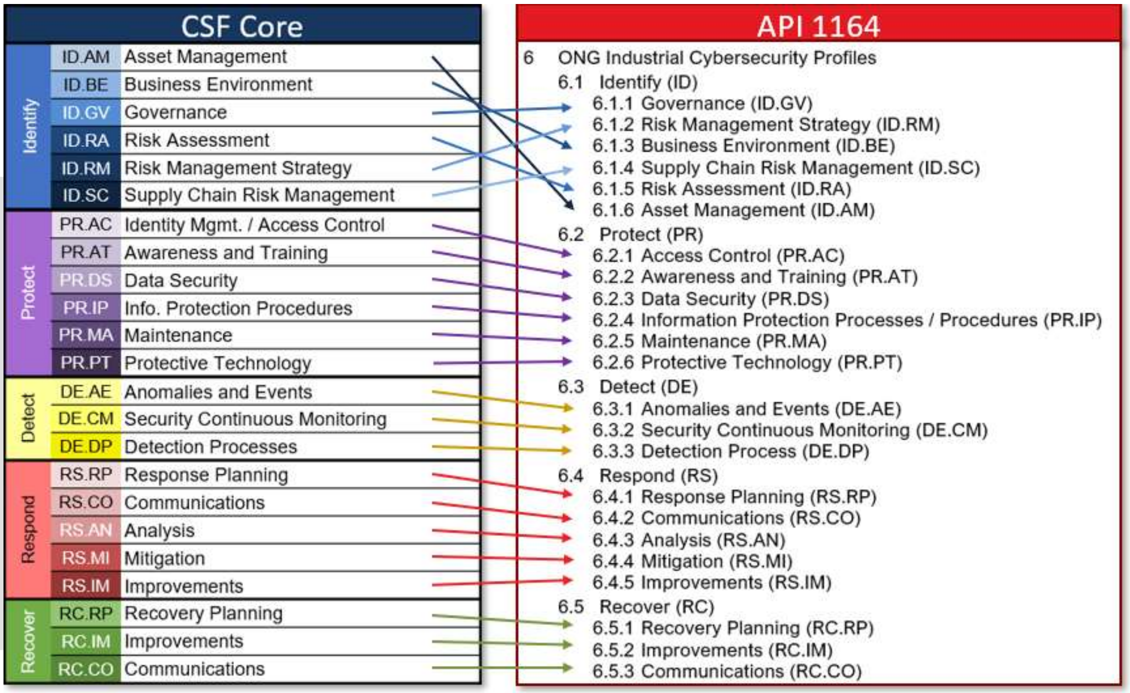
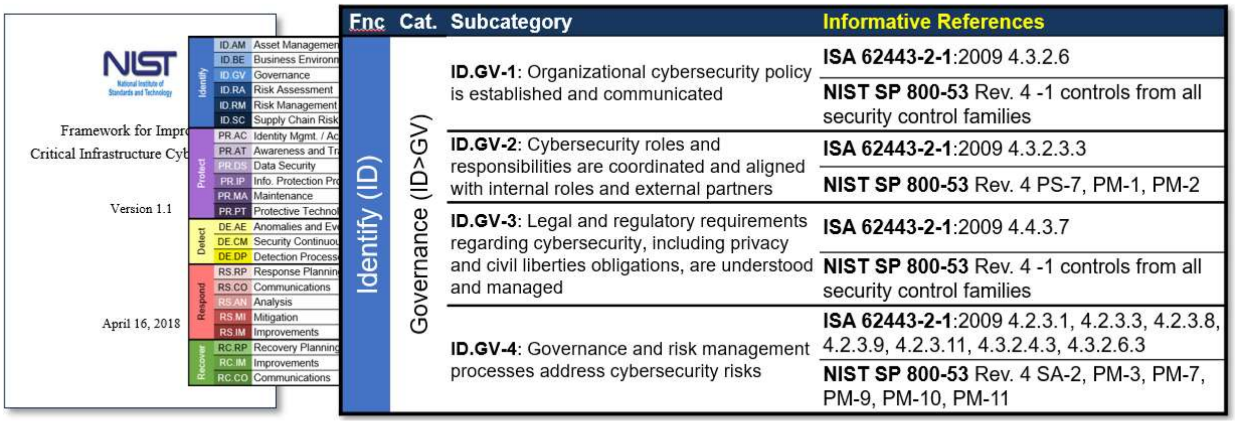

CSF Core
Identify
ID.AM Asset Management
ID.BE Business Environment
ID.GV Governance
ID.RA Risk Assessment
ID.RM Risk Management Strategy
ID.SC Supply Chain Risk Management
Protect
PR.AC Identity Mgmt. / Access Control
PR.AT Awareness and Training
PR.DS Data Security
PR.IP Info. Protection Procedures
PR.MA Maintenance
PR.PT Protective Technology
Detect
DE.AE Anomalies and Events
DE.CM Security Continuous Monitoring
DE.DP Detection Processes
Respond
RS.RP Response Planning
RS.CO Communications
RS.AN Analysis
RS.MI Mitigation
RS.IM Improvements
Recover
RC.RP Recovery Planning
RC.IM Improvements
RC.CO Communications
API 1164
6 ONG Industrial Cybersecurity Profiles
6.1 Identify (ID)
6.1.1 Governance (ID.GV)
6.1.2 Risk Management Strategy (ID.RM)
6.1.3 Business Environment (ID.BE)
6.1.4 Supply Chain Risk Management (ID.SC)
6.1.5 Risk Assessment (ID.RA)
6.1.6 Asset Management (ID.AM)
6.2 Protect (PR)
6.2.1 Access Control (PR.AC)
6.2.2 Awareness and Training (PR.AT)
6.2.3 Data Security (PR.DS)
6.2.4 Information Protection Processes / Procedures (PR.IP)
6.2.5 Maintenance (PR.MA)
6.2.6 Protective Technology (PR.PT)
6.3 Detect (DE)
6.3.1 Anomalies and Events (DE.AE)
6.3.2 Security Continuous Monitoring (DE.CM)
6.3.3 Detection Process (DE.DP)
6.4 Respond (RS)
6.4.1 Response Planning (RS.RP)
6.4.2 Communications (RS.CO)
6.4.3 Analysis (RS.AN)
6.4.4 Mitigation (RS.MI)
6.4.5 Improvements (RS.IM)
6.5 Recover (RC)
6.5.1 Recovery Planning (RC.RP)
6.5.2 Improvements (RC.IM)
6.5.3 Communications (RC.CO)

**Figure 1-2: CSF Core mapping to Pipeline Target Profile Requirements**

This realignment with the details of specific activities and outcomes does not come directly from the Framework Core categories and subcategories. The Framework Core also specifies Informative references. These references were used, specifically focusing on industrial cybersecurity requirements, as a foundation to the content of this Standard.


NIST
National Institute of Standards and Technology
Framework for Impr
Critical Infrastructure Cyb
Version 1.1
April 16, 2018
Identify
ID.AM Asset Managemen
ID.BE Business Environn
ID.GV Governance
ID.RA Risk Assessment
ID.RM Risk Management
ID.SC Supply Chain Risk
Protect
PR.AC Identity Mgmt. / Ac
PR.AT Awareness and Tr
PR.DS Data Security
PR.IP Info. Protection Pr
PR.MA Maintenance
PR.PT Protective Technol
Detect
DE.AE Anomalies and Ev
DE.CM Security Continuou
DE.DP Detection Process
Respond
RS.RP Response Plannin
RS.CO Communications
RS.AN Analysis
RS.MI Mitigation
RS.IM Improvements
Recover
RC.RP Recovery Planning
RC.IM Improvements
RC.CO Communications

| Fnc | Cat. | Subcategory | Informative References |
|---|---|---|---|
| Identify (ID) | Governance (ID>GV) | **ID.GV-1**: Organizational cybersecurity policy is established and communicated | **ISA 62443-2-1**:2009 4.3.2.6<br>**NIST SP 800-53** Rev. 4 -1 controls from all security control families |
| | | **ID.GV-2**: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners | **ISA 62443-2-1**:2009 4.3.2.3.3<br>**NIST SP 800-53** Rev. 4 PS-7, PM-1, PM-2 |
| | | **ID.GV-3**: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | **ISA 62443-2-1**:2009 4.4.3.7<br>**NIST SP 800-53** Rev. 4 -1 controls from all security control families |
| | | **ID.GV-4**: Governance and risk management processes address cybersecurity risks | **ISA 62443-2-1**:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3<br>**NIST SP 800-53** Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 |

**Figure 1-3: NIST CSF Informative References**

### 1.3.3 NIST Cyber Security Framework Extensions

This standard significantly extended the Framework's Informative References by partnering with the International Society of Automation (ISA). ISA graciously permitted a non-distributable, limited use copy of the two *ISA 62443 Security for Industrial Automation and Control Systems* documents specified in the Informative References, and four additional documents in the ISA 62443 series, not referenced in the NIST Framework, to be used as a reference during the creation of this Standard. Implementors of this Standard may find it useful to review for context, background, and general IAC security considerations the entire ISA 62443 series directly, especially related to the primary IAC security elements of zones and conduits. The implementor may want to obtain a licensed copy prior to implementing this Standard.

The Framework's Informative References from NIST SP 800-53r4 were used to map to the NIST SP 800-82r2 Guide to Industrial Control Systems (ICS) Security for ICS specific guidance on the applicability and implementation context of the 800-53r4 elements referenced. This required multiple passes between 800-53r4 and 800-82r2 to produce an actionable item.

### 1.3.4 Content Mapping

The requirements, activities, and outcomes from the Framework's informative references and the additional standards were then augmented and enriched to address the tailored context. This included incorporating the cybersecurity measures specified in TSA's Pipeline Security Guidelines.

This filtering, selection, alignment, and the augmentation and enrichment of contextual implementation guidance of this Standard's cybersecurity activities and outcomes is depicted in Figure 1-4

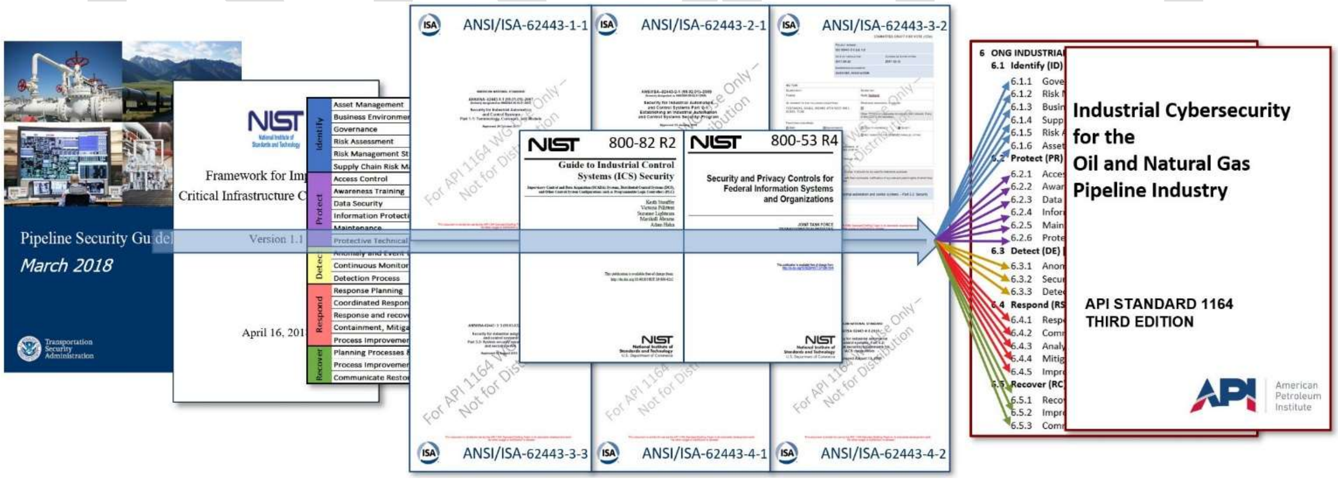


**Figure 1-4: API 1164 Content Creation Mapping**

### 1.3.5 Document Structure

- **Section 2: Normative References**
- **Section 3: Terms, Definitions, Acronyms, and Abbreviations**
  Provides definitions for Terms, Definitions, Acronyms, and Abbreviations used in this standard or that are relevant to understanding the background, context or a concept covered by this standard.
- **Section 4: ONG Pipeline IAC Cybersecurity Profiles**
  This section sets the foundation of pipeline IAC cybersecurity. It introduces the concept of three (3) different security profiles mapped to 3 levels of threat protection objectives. This section also sets the foundational concepts of IAC cybersecurity common constraints of IAC essential functions and safety instrumented systems considerations. Also defined in this section are six (6) common pipeline industry business objectives and a mapping of those business objectives to each NIST CSF Function, Category, and subcategory. Lastly, this section maps the business objective impacts to threat protection objectives and then maps those threat protection objectives to security profiles.
- **Section 5: ONG IAC Cybersecurity Policy, Plans, and Program**
  This section defines how to implement this standard. It builds on the foundation set in Section 4 by defining an IAC cybersecurity management system mandated by a company policy and documented in an IAC Cybersecurity Plan. The IAC Cybersecurity Plan has a cornerstone of risk management,

including a risk strategy, risk assessment processes, and risk responses aligned to the risk strategy. The IAC Cybersecurity Policy and the IAC Cybersecurity Plan elements are defined as a set of requirements based on applicable security profiles. This section also defines the concepts of segregating IAC Cyber assets into cybersecurity zones and connecting those zones using cybersecurity conduits. It also defines how to perform business objective impacts assessments to select applicable security profile requirements for the IAC Cybersecurity Zones and IAC Cybersecurity Conduits.

- **Sections 6 - 10: ONG IAC Cybersecurity Profile Requirements**
  These sections specify the cybersecurity requirements for the three cybersecurity profiles that are to be applied to the IAC Security Zones and IAC Security Conduits based on their business impact severity level.

- **APPENDIX A: ANNEX A**
- **Business Objectives to API 1164 Control Subcategories**
  This appendix identifies key cybersecurity practices for supporting the pipeline business objectives. This allows the implementor to focus on implementing those cybersecurity measures against threats that could severely compromise the pipeline's essential mission.

# 2 Normative References

This document contains no normative references. A list of documents and articles associated with API 1164 are included in the bibliography.

# 3 Terms, Definitions, Acronyms, and Abbreviations

## 3.1 Terms and Definitions

**3.1.1**
**asset**
An object represented either physically, logically, or virtually, that is owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization.

**3.1.2**
**attack vector**
A path or a means by which unauthorized access can be gained to a device or a network for malicious purposes.

**3.1.3**
**boundary device**
Communication asset residing in either a security zone or security conduit, which provides an interface between a zone and the conduit.

**3.1.4**
**cyber asset**
A physical or virtual device with the following minimum resources: 1) digital logic processing capability (e.g. CPU, ASIC); 2) memory (volatile or permanent); 3) one communications port, which is used in IT or industrial automation control solutions.

**3.1.5**
**cybersecurity plan**
One or more formal documents that specify all the requirements and outcomes of a Cybersecurity Program.

**3.1.6**
**cybersecurity policy**
A high-level document that describes the overall security goals and defines requirements for "what" is done by "whom", to effectively manage cybersecurity risks.

**3.1.7**
**cybersecurity program**
An operationalized Cybersecurity Plan which includes the people operating in the context of their roles and responsibilities, processes that drive cybersecurity outcomes - including the effectiveness and performance measurements of those outcomes, and the technologies that support the people and processes all intended to manage the cybersecurity risk.

**3.1.8**
**external zone**
A network outside the purview of an IAC Cyber Environment, controlled and managed by a separate legal entity, partner, vendor, supplier, joint-venture entity, or another function within the organization.

**3.1.9**
**IAC audit record**
The evidentiary artifact of the occurrence of an IAC Security Audit Event.

**3.1.10**
**external IAC transport service**
A network segment, which is part of an IAC Internal Conduit, that is responsible for delivering IAC data to the application processes on host computers but is outside the purview of an IAC Cyber Environment, controlled and managed by a separate legal entity, partner, vendor, supplier, joint-venture entity, or another function within the organization. (e.g. 3rd party satellite service; corp. owned and managed microwave backbone).

**3.1.11**
**IAC cyber asset**
A Cyber Asset within the security perimeter of an IAC Segregated Environment.

**3.1.12**
**IAC cyber environment**
Any combination of two or more IAC Cyber Assets, IAC Cyber Systems, IAC Security Zones, or IAC Security Conduits being considered collectively. The scope can be as large as enterprise wide (e.g. all IAC Cyber Assets for all pipelines), or as constrained as two IAC Cyber Assets under joint consideration.

NOTE Depending on the contextual use, the scope may refer to organization's entire IAC Cyber Environment as segmented and segregated, a subset of the organization's IAC environment as segmented and segregated, or a single IAC Segregated Environment (a Security Zone or a Security Conduit, or a zone conduit pair).

**3.1.13**
**IAC cyber solution**
One or more IAC Cyber Assets integrated collectively into a single solution deployed within an IAC Security zone, or IAC Security Zone Conduit, providing essential functions.

**3.1.14**
**IAC cyber system**
A single IAC Cyber Asset or a grouping of IAC Cyber Assets distinguished as a single entity, designed to perform a discernably separate set of IAC essential functions.

**3.1.15**
**IAC cybersecurity plan**
A cybersecurity plan scoped exclusively for IAC Cyber Environments, which addresses specific IAC cybersecurity and IAC operational requirements, constraints, and considerations when defining an IAC Cybersecurity Program.

**3.1.16**
**IAC cybersecurity policy**
A cybersecurity policy that describes the overall IAC cybersecurity goals and objectives, is approved by organizational leadership, and authorizes, mandates, or otherwise wills into existence an IAC Cybersecurity Program to achieve those goals.

**3.1.17**
**IAC cybersecurity profile**
A collection of defined IAC cyber activities and desired outcomes (Functions, Categories, Subcategories, procedures, practices, and controls) that manages risk to mission/business objectives and are bounded by the constraints and requirements of a particular scenario.

**3.1.18**
**IAC cybersecurity program**
An operationalized IAC Cybersecurity Plan which includes the people operating in the context of their roles and responsibilities, processes that drive cybersecurity outcomes, including the effectiveness and performance measurements of those outcomes, and the technologies that support the people and processes to manage the cybersecurity risk.

**3.1.19**
**IAC essential function**
An industrial automation and control function that provides a capability that is required to maintain health, safety, the environment, and availability for the process under control. Essential functions include at least the following three categories: 1) Protection: Functions performed by a Safety Instrumented System (SIS), 2) Control: Functions controlling a process and/or equipment; 3) View: The ability of the operator to view and manipulate the equipment under control

NOTE All uses of the term "essential function", where not otherwise qualified, should be assumed to refer to an IAC Essential Function.

**3.1.20**
**IAC external conduit**
An IAC Security Conduit that connects an External Zone and an IAC Intermediate Zone to provide security control and protection.

NOTE See Section 5.4.1 Defining IAC Segregated Environments: Security Zones and Conduits on page 17 below for clarification of security zones and security conduits.

**3.1.21**
**IAC intermediate conduit**
An IAC Security Conduit that connects to an IAC Intermediate Zone and an IAC Internal Zone to provide security control and protection.

**3.1.22**
**IAC intermediate zone**
An IAC Security Zone that connects to an External Zone using an IAC External Conduit and connects to an IAC Internal Zone using an IAC Intermediate Conduit to indirectly present IAC data and services and for providing external controlled access to IAC services by external users to an IAC Security Zone.

**3.1.23**
**IAC internal conduit**
A Security Zone Conduit that connects an IAC Internal Zone to a separate IAC Internal Zone.

**3.1.24**
**IAC internal zone**
A single IAC Cyber Asset or a grouping of IAC Cyber Assets that implement a single level IAC cybersecurity profile and only communicates with other cyber assets not in the IAC Security Zone using an IAC Security Conduit.

**3.1.25**
**IAC security audit event**
A security audit event generated from an IAC Cyber Asset, IAC Security Zone, or an IAC Security Conduit.

**3.1.26**
**IAC security conduit**
A Security Conduit used in an IAC Cyber Environment including (*all*) IAC External Conduit(s), IAC Intermediate Conduit(s), and IAC Internal Conduit(s).

NOTE When defining or referencing security requirements, the term "IAC Security Conduit" is to be interpreted that the security requirements are applicable to all IAC conduit types listed above in this definition.

**3.1.27**
**IAC security zone**
Security Zone used in an IAC Segregated Environment including IAC Internal Zone(s) and IAC Intermediate Zone(s).

NOTE When defining or referencing security requirements, the term "IAC Security Zones" is to be interpreted that the security requirements are applicable to all IAC zone types listed above in this definition.

**3.1.28**
**IAC segregated environment**
An IAC Security Zone (IAC Intermediate Zone or IAC Internal Zone) or an IAC Security Conduit (IAC External Conduit, IAC Intermediate Conduit, or IAC Internal Conduit), or a combination of any IAC Security Zone and IAC Security Conduit being considered collectively.

NOTE When defining or referencing security requirements, the terms “IAC Segregated Environment” and “IAC Segregated Environments” are to be interpreted as the security requirements are applicable to all IAC Security Zone and IAC Security Conduit types listed above in this definition.

**3.1.29**
**IAC support asset**
A Cyber Asset that is used in the maintenance, management, configuration, or administration of an IAC Cyber Asset, IAC Cyber System, or IAC Cyber Environment.

**3.1.30**
**impact**
A measure of the loss or harm associated with a consequence.

**3.1.31**
**network segmentation**
The process of dividing a network into separately managed parts.

**3.1.32**
**network segregation**
The process of defining different protection rulesets using risk-based criteria and implementing those rules to manage the security of a network segment.

**3.1.33**
**physical asset**
An asset that has mass, can be perceived through visual or tactile human senses.

**3.1.34**
**nonlocal access**
Human user communication with an IAC Cyber Asset using a network connection whether originating from within the same IAC Security Zone as the IAC Cyber Asset or a different security zone, including an External Security Zone.

**3.1.35**
**risk management strategy**
A documented declaration of an organization’s risk priorities (e.g. importance of missions/business functions and trade-offs between varying types of risk), constraints on the risk assessment, response and monitoring alternatives, risk tolerances (e.g. levels and types of risk, and degree of risk uncertainty that are acceptable), and assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time.

**3.1.36**
**security audit event**
Any observable occurrence in a Cyber Asset which is significant and relevant to the security of the Cyber Asset and the environment in which that asset operates to meet specific and ongoing audit needs.

**3.1.37**
**security conduit**
A Security Zone that is specific to communication processes, containing logical grouping of assets that are used in, perform, monitor, and defend communications between Security Zones.

**3.1.38**
**security perimeter**
Logical boundary encompassing all the cyber assets that can communicate with each other without use of a Security Conduit.

NOTE The security perimeter may mirror a physical boundary of a facility or site for convenience or practical implementation reasons but that is coincidental to a Security Zone’s purpose and use.

**3.1.39**
**security zone**
A grouping of cyber assets that adhere to the same security controls, whose security posture is managed collectively, and only communicates with other Cyber Assets outside the Security Perimeter using a Security Conduit.

**3.1.40**
**threat**
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

**3.1.41**
**vulnerability**
A flaw or weakness in computer system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [NIST SP 800-47]

## 3.2 Acronyms

| | |
|---|---|
| CSF | NIST Cyber Security Framework |
| CFR | Code of Federal Regulation |
| DOT | US Department of Transportation |
| FERC | Federal Energy Regulatory Commission |
| HSE | Health Safety and Environment |
| IAC | Industrial Automation and Control |
| IIoT | Industrial Internet of Things |
| ISA | International Society of Automation |
| NIST | National Institute of Standards and Technology |
| ONG | Oil and Natural Gas Industry |
| PHMSA | Pipeline and Hazardous Materials Safety Administration |
| TSA | Transportation Security Administration |

# 4 ONG Pipeline IAC Cybersecurity Profiles

## 4.1 IAC Cybersecurity Profile - Introduction

The NIST CSF defines a Profile as a representation of the outcomes based on business needs that an organization has selected from the CSF Categories and Subcategories. It can be characterized as the alignment of the policies, procedures, and practices to the Functions, Categories, and Subcategories for a particular scenario.

Within the context of this Standard, an API 1164 Profile is a collection of selected cybersecurity activities and desired outcomes (Functions, Categories, Subcategories, and security requirements) for a particular scenario. The selection is based on certain constraints and business/mission objectives.

API 1164 specifies multiple profiles for different scenarios. These profiles provide actionable approaches to managing IAC cybersecurity risk. They define a set of requirements and cyber activities that are designed to drive outcomes to manage the potential risk to business mission and objectives of the ONG pipeline industry. They are customized for natural gas and hazardous liquid transmission pipelines, natural gas distribution pipeline systems, liquefied natural gas facilities, and others involved in these industries.

### 4.1.1 Scenario Profiles

This document defines the following three scenario profiles.

#### 4.1.1.1 Baseline Profile

This profile covers IAC Cybersecurity Program wide cyber activities and outcomes for all business objectives for the ONG Pipeline industry. It also specifies IAC Cybersecurity activities and outcomes for the IAC Segregated Environments with the potential for low impact to the pipeline industry business objectives.

#### 4.1.1.2 Enhanced Profile

This profile includes API 1164 Baseline Profile cyber activities and outcomes plus the IAC Cybersecurity activities and outcomes for IAC Segregated Environments with the potential for a medium level impact to the pipeline industry business objectives.

#### 4.1.1.3 Extended Profile

This profile includes the API 1164 Enhanced Profile cyber activities and outcomes plus IAC Cybersecurity activities and outcomes for IAC Segregated Environments with the potential for the highest-level impact to the pipeline industry business objectives.

## 4.2 IAC Cybersecurity Profile - Common Constraints

The IAC cybersecurity requirements detailed in Sections 6 through 10 have been developed based on common constraints applicable to cyber activities and outcomes for all API 1164 profiles. The IAC environment fits underneath the broad designation of Operational Technology (OT) rather than Information Technology (IT) despite the usage of elements that are often associated with traditional IT environments. This key difference is not necessarily based on the technology deployed but rather the intent of the environment and the impact of threats to the environment. IT environments are dynamic in function and generally serve business communication/decision making purposes where threats to confidentiality and integrity are most significant.

OT environments, on the other hand, are often considered deterministic meaning specific control action results from a specific input and is always expected to produce the same action. Any security threat to an OT environment’s ultimate availability threatens its basic design criteria. The IAC cybersecurity requirements outlined in this document are defined with the control system security attributes of availability first and integrity second with confidentiality following. These security attributes are further prioritized through the lens of safety before operational considerations. Correct prioritization of the protection and support of essential functions provided by the IAC is foundational to a holistic risk-based approach to IAC cybersecurity activities.

### 4.2.1 Prioritizing Control System Essential Functions

An IAC function is essential when the capability is required to maintain health, safety, the environment, and availability for the equipment under control. Essential functions include but are not limited to: functions performed by a Safety Instrumented System (SIS) (Loss of Protection), the functions controlling a process and/or equipment (Loss of Control) and the ability of the operator to view / manipulate the equipment under control (Loss of View).

Prioritization of IAC security activities and outcomes should always be in support of the IAC essential functions they are designed to protect. Any security activity or outcome that could result in the decrease of availability or integrity of an essential function is an improperly prioritized security capability, and thereby ill-conceived.

### 4.2.2 Safety Instrumented Systems Considerations

Although SIS is outside the scope of this document, the tenet of Safety-First mandates that special considerations should be taken to ensure SIS functions are not inadvertently impacted.

Control system cybersecurity outcomes, processes, and cybersecurity controls should include considerations of potential impact to SIS functions. These include, but are not limited to:

- IAC Risk Assessments
- Cybersecurity Control Design
- Cybersecurity Control Implementation
- Cybersecurity Control Testing

## 4.3 IAC Cybersecurity Profile - Threat Protection Objectives

The IAC cyber activities and outcomes defined for each of the three (3) API 1164 profiles are designed to meet threat protection objectives.

These protection objectives are defined to defend against increasing levels of threat factors, including resourcing, sophistication, motivation, knowledge, and skill. These threat protection objectives are mapped to the different levels of potential impact to pipeline industry business mission and objectives. The higher the level of potential impact the higher the profile for a higher level of protection against a higher level of threat factors.

The Threat Protection Objective to API 1164 Profile mapping is detailed in Table 4-1 below.

| API 1164 Profile | Threat Rating | Threat Protection | Threat Protection Objective |
|---|---|---|---|
| P3 Extended | T3 | Advanced | Protect for a deliberate attack that is highly motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge. |
| P2 Enhanced | T2 | Heightened | Protect for a deliberate attack that is moderately motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge. |
| P1 Baseline | T1 | Basic | Protect for a deliberate attack that is simple, low resourced and motivated and does not leverage any specific skills. |
| | | | Protect for unintentional or coincidental security violation. |

**Table 4-1: API 1164 Security Level Threat Protection Objectives**

## 4.4 IAC Cybersecurity Profile - Business and Mission Objectives

The development of an Industry IAC Cybersecurity Profile includes the identification of common business and mission objectives for that industry. These business and mission objectives provide the necessary context for identifying and managing applicable cybersecurity risk mitigation.

### 4.4.1 Pipeline Industry Business and Mission Objectives

There are six (6) shared business and mission objectives for the ONG pipeline sector identified within this standard. Other business and mission objectives likely exist in individual companies, industry sectors, and/or industry subsectors, but they are left up to the stakeholder company to address as appropriate and aligned to policies, procedures, and priorities.

#### 4.4.1.1 Maintain Human Health and Safety

Manage cybersecurity risks that could potentially impact human safety, including both accidental and deliberate hazards. Cybersecurity risk on the pipeline system can adversely affect human safety. Personnel should understand cybersecurity and safety interdependencies. Cybersecurity measures are not allowed to adversely affect control system essential functions, especially loss of protection that could result in human safety consequences.

#### 4.4.1.2 Maintain Environmental Safety

Manage cybersecurity risks that could negatively impact the environment. This includes both accidental and deliberate damage. Cybersecurity risk on the pipeline system can adversely affect environmental safety. Personnel should understand cybersecurity and environmental safety interdependencies. Cybersecurity measures must not adversely affect control system essential functions, especially loss of protection that could result in environmental safety consequences.

#### 4.4.1.3 Maintain Property Safety

Manage cybersecurity risks that could negatively impact the safety to property both owned by the company and property owned by others. This includes both accidental and deliberate damage. Cybersecurity risk on the pipeline system can adversely affect property safety. Personnel should understand cybersecurity and property safety interdependencies. Cybersecurity measures must not adversely affect control system essential functions, especially loss of protection that could result in property safety consequences.

#### 4.4.1.4 Maintain Operational Capability

Manage cybersecurity risks that could adversely affect delivery and other contractual commitments. Cybersecurity risk within the IAC Cyber Environment, including asset damage, can adversely affect the essential functions impacting the ability to realize commercial obligations. Personnel should understand cybersecurity and commercial commitment interdependencies

#### 4.4.1.5 Maintain Compliance Posture

Manage cybersecurity risks that could impact a compliant posture with regulatory, legal, and corporate policy requirements. Although, there are some shared regulatory requirements between hazardous liquids and natural gas pipeline, there are also unique requirements.

#### 4.4.1.6 Maintain Reputation

Manage cybersecurity risks that could adversely affect the company's reputation or generate negative publicity. Reputation damage exposure can occur at the international, national, regional, or local levels. The scope of the reputation damage can be with the public, governments, regulatory bodies, industry, or with one of more customers. Protect against compromise of the availability and integrity of the control process and associated data.

### 4.4.2 Security Requirements to Business Objectives Mapping

To align cybersecurity goals with overall business mission, the Profile subcategories are prioritized to support specific business objectives. Key cybersecurity practices are identified for supporting each business and mission objective, allowing individual companies to better prioritize actions and resources. This allows the implementor to focus on implementing those cybersecurity measures against threats that could severely compromise the pipeline's essential mission. Table 4-2 below depicts the overview of mapping CSF subcategories to common ONG pipeline industry business objective.

| Function | Maintain Human Health/Safety | Maintain Environmental Safety | Maintain Property Safety | Maintain Operational Capability | Maintain Compliance Posture | Maintain Reputation |
|---|---|---|---|---|---|---|
| IDENTIFY | AM-1...SC-5 | AM-1...SC-5 | AM-1...SC-5 | AM-1...SC-5 | AM-1...SC-5 | AM-1...SC-5 |
| PROTECT | AC-1...PT-5 | AC-1...PT-5 | AC-1...PT-5 | AC-1...PT-5 | AC-1...PT-5 | AC-1...PT-5 |
| DETECT | AE-1...DP-5 | AE-1...DP-5 | AE-1…DP-5 | AE-1...DP-5 | AE-1...DP-5 | AE-1...DP-5 |
| RESPOND | RP-1...IM-2 | RP-1...IM-2 | RP-1...IM-2 | RP-1....IM-2 | RP-1…IM-2 | RP-1...IM-2 |
| RECOVER | RP-1...CO-3 | RP-1...CO-3 | RP-1...CO-3 | RP-1...CO-3 | RP-1...CO-3 | RP-1...CO-3 |
| | | | | | | |

**Table 4-2: API 1164 Security Level Threat Protection Objectives**

See ANNEX A

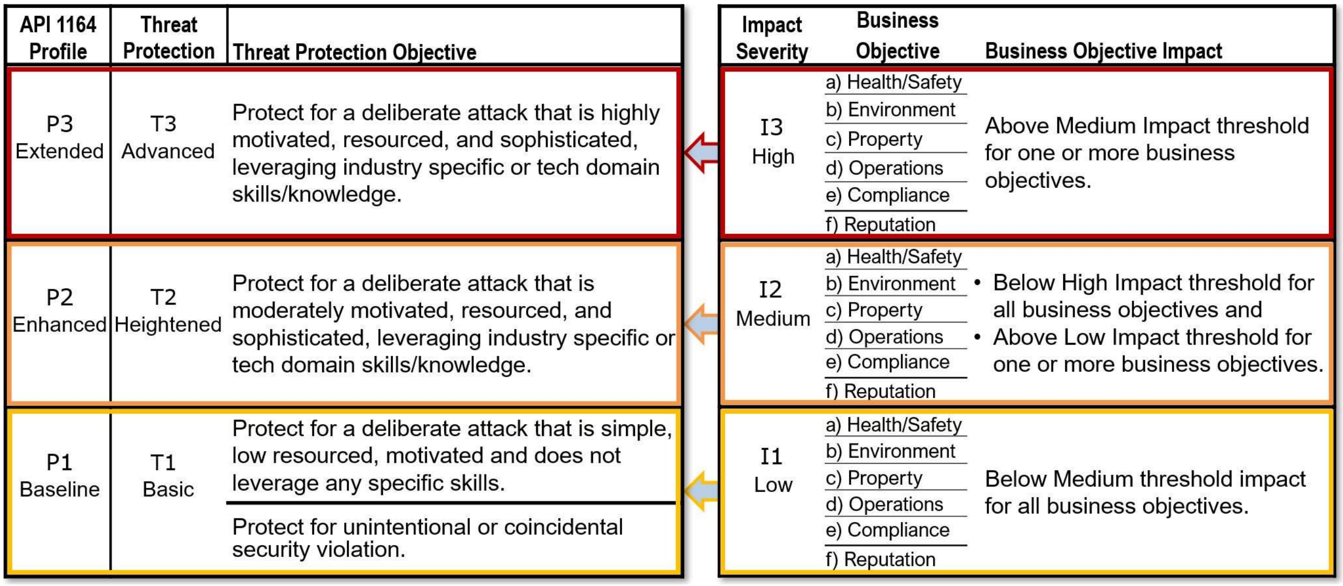
Business Objectives to API 1164 **Control Subcategories** on page 1 below for the detailed mapping of API 1164 control subcategories to business objectives.

## 4.5 Profile Mapping - Business Objective Impact to Threat Protection Level

For this Standard to appropriately scope and prioritize the ONG pipeline IAC cybersecurity activities and outcomes into scenario-based Profiles, it is essential the potential impacts to pipeline business objectives are mapped to appropriate threat protection levels.

API 1164 categorizes the impact to pipeline business objectives from Cybersecurity hazards into three levels, I1, I2, and I3. These three levels correspond to the three Threat Protection Objectives.

Figure 4-1 below details the Profile to Business Objective Impact Severity mapping:



| API 1164 Profile | Threat Protection | Threat Protection Objective |
|---|---|---|
| P3<br>Extended | T3<br>Advanced | Protect for a deliberate attack that is highly motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge. |
| P2<br>Enhanced | T2<br>Heightened | Protect for a deliberate attack that is moderately motivated, resourced, and sophisticated, leveraging industry specific or tech domain skills/knowledge. |
| P1<br>Baseline | T1<br>Basic | Protect for a deliberate attack that is simple, low resourced, motivated and does not leverage any specific skills.<br>Protect for unintentional or coincidental security violation. |

| Impact Severity | Business Objective | Business Objective Impact |
|---|---|---|
| I3<br>High | a) Health/Safety<br>b) Environment<br>c) Property<br>d) Operations<br>e) Compliance<br>f) Reputation | Above Medium Impact threshold for one or more business objectives. |
| I2<br>Medium | a) Health/Safety<br>b) Environment<br>c) Property<br>d) Operations<br>e) Compliance<br>f) Reputation | • Below High Impact threshold for all business objectives and<br>• Above Low Impact threshold for one or more business objectives. |
| I1<br>Low | a) Health/Safety<br>b) Environment<br>c) Property<br>d) Operations<br>e) Compliance<br>f) Reputation | Below Medium threshold impact for all business objectives. |

**Figure 4-1: API 1164 Business Objective Impact Mapping to Threat Protection Profiles**

The following section details the use of the Business Objective Impact table and the selection of cybersecurity profile requirements.

# 5 ONG IAC Cybersecurity Policy, Plans, and Program

This Standard promotes tailoring of its requirements based on an implementor's unique priorities of the common ONG pipeline business objectives. It also supports customizing the selection of a requirement or its implementation specifics when supported by a risk assessment that has considered alternate applicable mitigating controls and circumstances as part of the company's documented risk management processes. This tailoring provides flexibility for easier implementation across the in-scope disparate environments, resourcing constraints, and risk postures.

However, implementors are not to simply select specific cybersecurity activities or outcomes that address gaps in their current profile. An organizationally approved Cybersecurity Policy is the cornerstone and authorization for all other cybersecurity components and activities including mandating an Industrial Cybersecurity Program be defined by a formal plan. Without these underlying foundational elements, the resulting ad hoc IAC cybersecurity activities will not be repeatable, measurable, nor maintainable and the IAC cybersecurity posture will erode over time.

This standard is written and only intended to be implemented using a top-down, hierarchal, and building block approach. This approach requires that foundational elements be specified first, followed by primary-elements and then secondary-elements, etc. The pipeline IAC Cybersecurity Baseline Profile is the foundation profile that covers IAC Cybersecurity Program wide cyber activities and outcomes.

The successful implementation of this Standard is founded on having executive sponsorship to ensure sufficient resources are committed and activities receive appropriate priority. This sponsorship comes in the form of an approved IAC Cybersecurity Policy. An approved IAC Cybersecurity Policy may be a separate policy document or may be incorporated in an overarching corporate cybersecurity policy. Because the scope of this document is constrained to IAC environments it is only concerned with the IAC elements of the cybersecurity policy. This document refers to IAC policy elements collectively as the IAC Cybersecurity Policy, whether implemented in a separate IAC document or incorporated in a larger scoped policy document.

This IAC Cybersecurity Policy is the cornerstone and authorization for all other API-1164 IAC cybersecurity components and activities. The Policy specifies the requirements for and mandates the implementation of a risk-based IAC Cybersecurity Program to manage the IAC Cyber Environment to a level of cyber risk deemed acceptable by the organizational leadership responsible for enterprise risk. The Policy mandates that the Program be defined by one or more formally documented plans, identified in this standard as The IAC Cybersecurity Plan.

As with the IAC Cybersecurity Policy, the IAC Cybersecurity Plan may be a single document or set of documents covering IAC cybersecurity activities and outcomes separately or may be incorporated in one or more overarching corporate cybersecurity plan documents. Because the scope of this document is constrained to IAC environments it is only concerned with the IAC elements of the cybersecurity plans. This document refers to the IAC plan elements collectively as the IAC Cybersecurity Plan, whether implemented in one or more separate IAC documents or incorporated in one or more larger scoped documents.The IAC Cybersecurity Plan specifies all the requirements, outcomes, and the foundational building elements, including the processes, roles and responsibilities of stakeholders, and vendor agnostic technologies required to operationalize the Industrial Cybersecurity Program. The IAC Cybersecurity program documentation hierarchy is depicted in Figure 5-1.

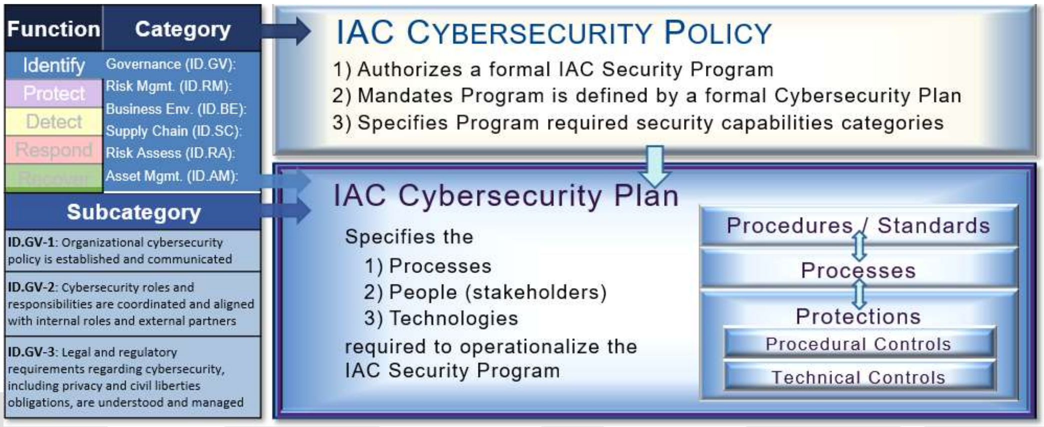

Function
Category
Identify
Protect
Detect
Respond
Recover
Governance (ID.GV):
Risk Mgmt. (ID.RM):
Business Env. (ID.BE):
Supply Chain (ID.SC):
Risk Assess (ID.RA):
Asset Mgmt. (ID.AM):
Subcategory
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-2: Cybersecurity roles 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
IAC CYBERSECURITY POLICY
1) Authorizes a formal IAC Security Program
2) Mandates Program is defined by a formal Cybersecurity Plan
3) Specifies Program required security capabilities categories
IAC Cybersecurity Plan
Specifies the
1) Processes
2) People (stakeholders)
3) Technologies
required to operationalize the IAC Security Program
Procedures / Standards
Processes
Protections
Procedural Controls
Technical Controls

**Figure 5-1: API 1164 CSF Sources for IAC Cybersecurity Policy and Plan**

Within this standard, the IAC Cybersecurity Policy requirements are derived from the NIST CSF Functions and Category elements. The requirements for the IAC Cybersecurity Plan is derived from the NIST CSF Category and Subcategories, Informative References, and extended references specified in section 1.3.3 NIST Cyber Security Framework Extensions on page 4 above.

This approach is consistent with TSA's Pipeline Security Guidelines cyber section NIST CSF mapping. It is also consistent with the TSA Pipeline Security Guidelines mandate that the Corporate Security Plan for each pipeline operator must include a Cyber System Security Plan. Within this document the cyber plan is referred to as the IAC Cybersecurity Plan.

## 5.1 IAC Cybersecurity Plan Development

The IAC Cybersecurity Plan is developed by engaging all stakeholders. It is aligned with the organization's control system architecture and information security architecture. Stakeholders can be internal or external to an organization.

To develop the IAC Cybersecurity Plan, a cross-functional team should be established consisting of key stakeholders engaged in the IAC design, engineering, implementation, execution, security, management, maintenance, operations or have a technical or process interdependency with the IAC Cyber Environment. In some organizations, it may be necessary for personnel to perform multiple roles. See Figure 5-2 for an example of a cross-functional team. It is also essential that stakeholders who provide or are involved in interfaces with the IAC Cyber Environment are members of the cross-functional team or, at minimum, are consulted and informed regarding the Plan's impact to those interfaces.

It is critical to program success that all stakeholders share their varied domain knowledge and experience to ensure the plan is comprehensive and considers all objectives, aspects, and constraints of the IAC Cyber Environment. Specifically, the cross-functional cybersecurity team should consider the impacts between IAC safety, essential functions, and security interdependencies.

The diagram below depicts the stakeholders that are either members of the cross-functional team or consulted during the creation or modification of the IAC Cybersecurity Plan.

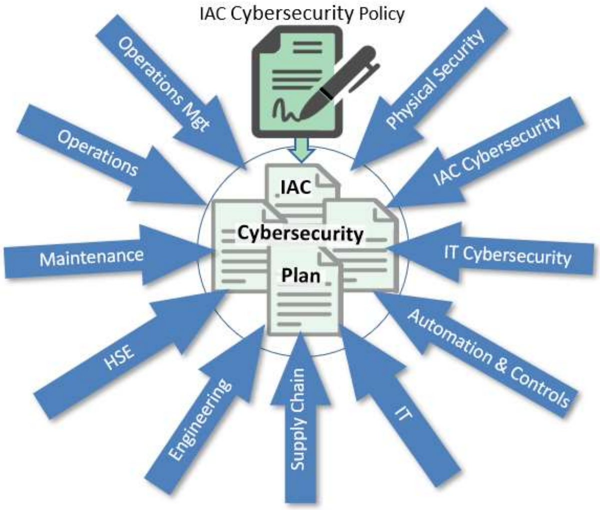


**Figure 5-2: IAC Cybersecurity Plan Development Participation**

## 5.2 IAC Cybersecurity Plan - Risk Management Foundation

Risk management is the foundational cybersecurity program capability to ensure resources are applied in a measured and appropriate way. A Risk Management Program is a collection of people, processes, and optional technology to systematically address risk, including cybersecurity risk, to organizational objectives (including mission, functions, image, reputation), organizational assets, individuals, and other organizations. It is based off a risk strategy, formally and consistently assesses risk, and formally and consistently responds to risk according to the organization's risk tolerance.

The intent of an effective API 1164 IAC Cybersecurity program is the management of risks associated with cybersecurity. While identification of impacts and necessary control mitigations is critical to the development of the program, evaluation of each from a risk perspective will ensure implementation of the program is appropriately executed and sustained consistent with an organization's risk posture.

A risk management process is comprehensive and requires the organization to:

1. Frame risk.
2. Assess risk.
3. Respond to risk once determined.
4. Monitor risk on an ongoing basis.

Risk management is carried out as a holistic, organization wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decisions are integrated into every aspect of the organization. Established risk management program elements are documented in the IAC Cybersecurity Plan, agreed to by organizational stakeholders and actively managed.

Managing cybersecurity risk, much like managing any organizational risk, is a complex activity that requires the involvement of the entire organization. Input from a variety of organizational sources such as leadership, operations, and support functions will ensure that risk is identified from a balanced perspective and is adequately tailored to meet the organizations specific cybersecurity needs.

An IAC Cybersecurity Risk Management Program has three (3) foundational elements that are defined in the IAC Cyber security Plan:

1. Risk Strategy.
2. Risk Assessment Process(es).
3. Predetermined Risk Response Matrix.

### 5.2.1 IAC Cybersecurity Plan - Risk Strategy

A risk management strategy is a formal element of a Risk Management Program. It is a documented framework that addresses how the organization intends to assess, respond to, and monitor risk. The risk management strategy is used to make consistent risk decisions based on predefined risk responses to asset classifications and risk levels.

The risk strategy contains the organization's

1. priorities (e.g. relative importance of business functions and trade-offs between varying types of risk),
2. constraints on the risk assessment,
3. response and monitoring alternatives,
4. risk tolerances (e.g. levels and types of risk, and degree of risk uncertainty that are acceptable), and
5. assumptions about the impact and the likelihood (threat and vulnerability factors) of occurrence that affect how risk is assessed, responded to, and monitored over time.

### 5.2.2 IAC Cybersecurity Plan - Risk Assessment

The purpose of the risk assessment process is to identify:

1. Threats to operations, assets, or individuals.
2. Vulnerabilities of Cyber Assets and ICS Cyber Assets.
3. The consequences/impact (i.e. harm) to the organization that may occur given the potential for threats exploiting vulnerabilities.
4. The likelihood that harm will occur.

The result is a determination of the cybersecurity risk's degree of harm and likelihood of harm occurring so the organization can understand the risk to organizational operations (including mission, functions, image, or reputation), assets, individuals, the upstream and downstream supply chain ecosystem, and to critical infrastructure.

### 5.2.3 IAC Cybersecurity Plan - Risk Response

There are four generally accepted responses to a risk:

1. Tolerate: The identified risk is below a company's risk tolerance. No action is needed or taken.
2. Treat: Remediate the identified risk such that the residual risk after remediation is at an acceptable level.
3. Terminate: Remove the identified risk. The residual risk is zero.
4. Transfer: The identified risk is moved to a third-party reducing residual risk to an acceptable level.

## 5.3 IAC Cybersecurity Plan - Operationalizing an IAC Cybersecurity Program

The IAC Cybersecurity Plan is operationalized, creating an IAC Cybersecurity Program, by implementing the procedures, processes, the procedural controls, and technical controls. Then the stakeholders in their varying capacities perform activities to interact and operate the plan elements. Stakeholders execute procedures, processes, procedural controls, and technical controls assigned to those roles.

A subset of those activities tests the effectiveness of the Program including both the design effectiveness and the operational effectiveness of the plan elements against program performance expectations and the outcomes aligned to the Plan's documented element objectives.

Based on the Program performance measures, improvements are recommended and prioritized. Often the recommendation is to improve the design or operations of the IAC Cybersecurity Plan documented elements. In certain situations, it is possible that the Policy requires modification to align to the operational reality of the IAC Security Program execution, a changing business environment or both. Improvement recommendations are reviewed to ensure alignment between IAC Cybersecurity Policy and the Plan allowing for modification of one or both. The API 1164 Policy and Plan driven IAC Cybersecurity Program model is shown in Figure 5-3 below.

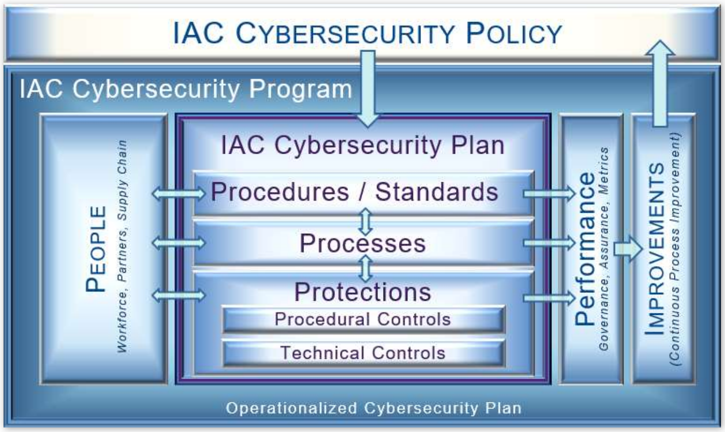

IAC Cybersecurity Policy
IAC Cybersecurity Program
People
Workforce, Partners, Supply Chain
IAC Cybersecurity Plan
Procedures / Standards
Processes
Protections
Procedural Controls
Technical Controls
Performance
Governance, Assurance, Metrics
Improvements
(Continuous Process Improvement)
Operationalized Cybersecurity Plan

**Figure 5-3: API 1164 Policy and Plan Driven IAC Cybersecurity Program**

## 5.4 IAC Cybersecurity Plan – Selecting Cybersecurity Profiles

Figure 5-4 below shows the API 1164 implementation process flow diagram that depicts how you use this standard to define your IAC Cybersecurity Plan using three different Cybersecurity Profiles. These three Cybersecurity Profiles are based on three (3) levels of threat protection objectives mapped to three (3) business objective impact severity levels.

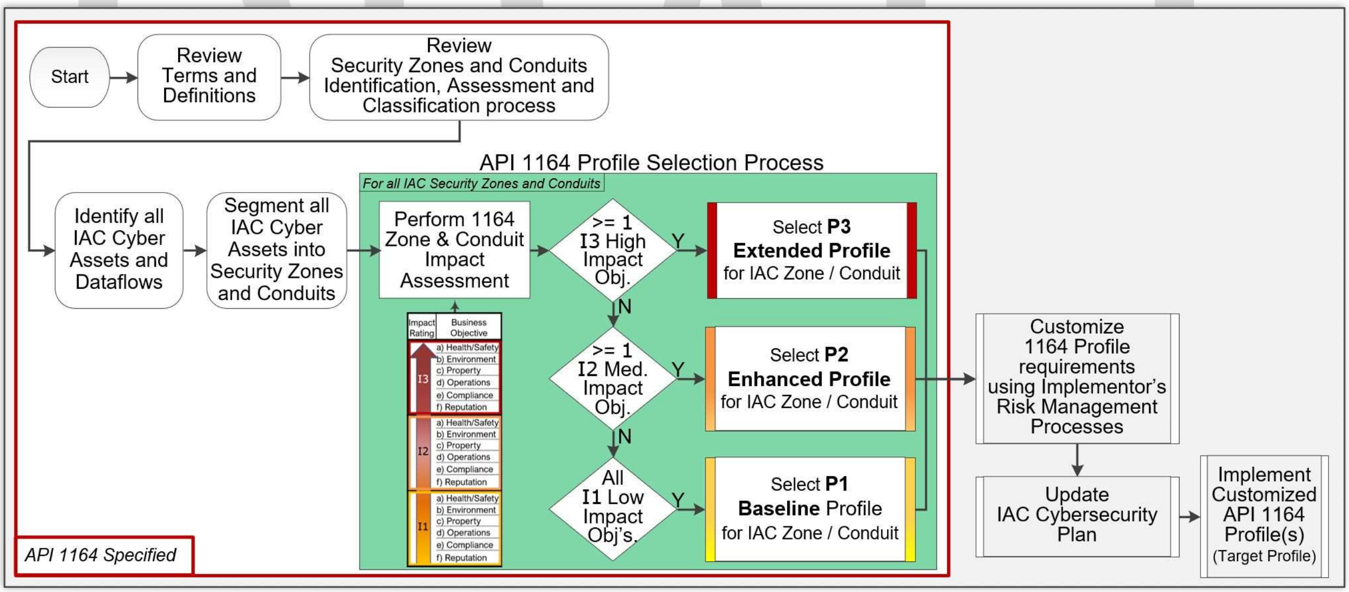

Start
Review Terms and Definitions
Review Security Zones and Conduits Identification, Assessment and Classification process
Identify all IAC Cyber Assets and Dataflows
Segment all IAC Cyber Assets into Security Zones and Conduits
API 1164 Profile Selection Process
For all IAC Security Zones and Conduits
Perform 1164 Zone & Conduit Impact Assessment
Impact Rating
Business Objective
I3
I2
I1
a) Health/Safety
b) Environment
c) Property
d) Operations
e) Compliance
f) Reputation
>= 1 I3 High Impact Obj.
>= 1 I2 Med. Impact Obj.
All I1 Low Impact Obj's.
Y
N
Select P3 Extended Profile for IAC Zone / Conduit
Select P2 Enhanced Profile for IAC Zone / Conduit
Select P1 Baseline Profile for IAC Zone / Conduit
Customize 1164 Profile requirements using Implementor's Risk Management Processes
Update IAC Cybersecurity Plan
Implement Customized API 1164 Profile(s) (Target Profile)
API 1164 Specified

**Figure 5-4: API 1164 Implementation Pattern**

NOTE This document specifies the items and activities in the red outlined section within the diagram above. It also provides guidance on the customization process in the grey but relies on the implementor's risk assessment process.

### 5.4.1 Defining IAC Segregated Environments: Security Zones and Conduits

#### 5.4.1.1 Network Segmentation and Network Segregation

Protecting network integrity is a foundational element of defending interconnected systems, especially within IAC Cyber Environments. A fundamental way to achieve this is through a defense-in-depth strategy that implements:

1. Network Segmentation: IAC network(s) are divided into separately managed segments.
2. Network Segregation: Different protection rulesets are defined using risk-based criteria and implemented to manage the security of each segment.

The combination of network segmentation and segregation is a key security countermeasure designed to compartmentalize devices where identified security practices are employed consistently to all cyber assets within the segment to achieve the desired cybersecurity target profile. The objective is to provide a segregated defense-in-depth approach to limit the attack surface of network interconnected IAC Cyber Assets from widespread horizontal and vertical expansion of a potential network intrusion.

The ISA-95 Enterprise Control System Integration, Part 1, based upon the Purdue Reference Model for CIM (hierarchical form), is widely known to serve as an example of effective deployment of the defense-in-depth concept for IAC Environments. While not endorsed or required by this standard, it can be used as a starting point for this phase of the API 1164 process.

#### 5.4.1.2 IAC Security Zones

An IAC Security Zone is a single IAC Cyber Asset, or a grouping of IAC Cyber Assets, identified as a single entity within a security perimeter. All IAC Cyber Assets within an IAC Security Zone implement shared security requirements distinguishing it from other Cyber assets with which they communicate. An IAC Security Zone has a clear logical border with other zones and the security of an IAC Security Zone is ensured by a combination of mechanisms both at the zone edge and within the zone.

An IAC Security Zone must have a clear logical or physical demarcation that may be defined by geographic boundaries, an organization's functional / departmental boundaries, common cyber functional capabilities or any other physical or logical grouping applicable to a given situation that will implement the common set of security controls on all assets within the zone's security parameter.

The combination of network segmentation and security ruleset segregation defines an IAC Security Zone. The security zone protection ruleset implements all human, device, and process access to the zone, zone communications ingress and egress protections and security posture elements within the security zone.

Establishing security zones by grouping IAC and related cyber assets using risk-based criteria, including, but not limited to, shared risk profile, physical or logical location, criticality of assets, operational function, physical and logical access requirements or responsible organization allows for risk-appropriate security measures to be applied. These measures are applied both within the security zone and to control and protect the communications into and out of the security zone.

This improves the IAC security posture by reducing attack surfaces, limits exposure of critical production assets, and facilitates implementation of least privilege by restricting movement between security zones. Using a risk-based approach focuses security monitoring and controls on the zones where they are most effective and improves detection and response capabilities.

#### 5.4.1.3 IAC Security Conduits

A rule of IAC Security Zones is that the IAC Cyber Assets contained within them are only allowed to communicate with IAC Cyber Assets outside their zone through an IAC Security Conduit. An IAC Security Conduit is a special Security Zone that is specific to communication processes, containing logical grouping of assets that are used in, perform, monitor, and defend communications for the IAC Security Zones to which it connects.

IAC Security Conduits, usually consisting of one of more cyber assets, are security zones in and of themselves for access control and configuration management protection requirements. This is differentiated from what and how data traverses the conduit.

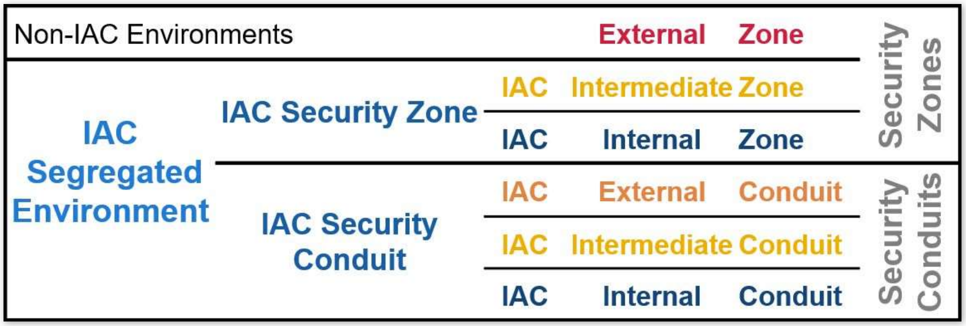
IAC Cyber Assets and the rules that govern the IAC Security Zone to which they belong determine what data will be communicated with other Security Zones. However, the IAC Security Conduit may control what data or services (e.g. communication protocols, TCP/IP Ports, etc.) can traverse the conduit. Therefore, the IAC Security Zone and the IAC Security Conduit work together to provide a layered defense-in-depth approach to IAC Security Zone data ingress and IAC Security Zone data egress.

The IAC Security Conduit may provide protection mechanisms in the form of access controls, data encryption, and the like while the data is traversing the IAC Security Conduit between the source IAC Security Zone and the target Security Zone. Edge and other network devices that create and manage the conduits create their own security zones that are risk-appropriately controlled on how they are managed and by whom.

Any boundary device of a security zone is an endpoint of a security conduit. Examples of devices that comprise a conduit include but are not limited to managed switches, routers, firewalls, 3rd party circuits, IDS, IPS, and other communication devices.

### 5.4.1.4 IAC Zone and Conduit Taxonomy

The use of Security Zones and Security Conduits within this standard are organized into a structured taxonomy to support consistency and understanding of the specific contexts in which Security Zone and Security Conduit requirements are defined and used. This is detailed in Table 5-1 below:



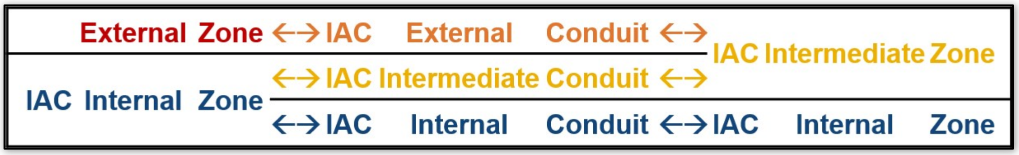
| | | | |
|---|---|---|---|
| Non-IAC Environments | | External Zone | Security Zones |
| IAC Segregated Environment | IAC Security Zone | IAC Intermediate Zone | |
| | | IAC Internal Zone | |
| | IAC Security Conduit | IAC External Conduit | Security Conduits |
| | | IAC Intermediate Conduit | |
| | | IAC Internal Conduit | |

**Table 5-1: API 1164 Security Zone and Security Conduit Taxonomy**

1. **Security Zones**:
   a. External Zone: A network segment outside the purview of an IAC Cyber Environment, controlled and managed by a separate legal entity, partner, vendor, supplier, joint-venture entity, or another function within the organization.
   b. IAC Security Zone: A Security Zone defined within an IAC Cyber Environment that requires the same security ruleset to be applied to all IAC Cyber Assets within its security perimeter. There are two (2) subtypes of IAC Security Zones:
      I. *IAC Intermediate Zone*: An IAC Security Zone that implements a single security ruleset for the purposes of indirectly presenting IAC data and services to an External Zone and for providing external controlled access to IAC services by users from an External Zone. IAC Cyber Assets within an IAC Intermediate Zones do not perform IAC essential functions.
      II. *IAC Internal Zone*: A single IAC Cyber Asset or a grouping of IAC Cyber Assets that implement a single security ruleset and only communicate with IAC Cyber Assets within the IAC Internal Zone, IAC Cyber Assets in another IAC Internal Zone, or IAC Cyber Assets in an Intermediate Zone.
2. **Security Conduits**: There are three (3) subtypes of IAC Security Conduits:
   a. IAC External Conduit: A Security Conduit that connects an External Zone with an IAC Intermediate Zone.
   b. IAC Intermediate Conduit: A Security Conduit that connects an IAC Intermediate Zone with an IAC Internal Zone.
   c. IAC Internal Conduit: A Security Conduit that connects an IAC Internal Zone with another IAC Internal Zone.

NOTE The scope of this document only includes IAC Security Conduits and within this document, Security Conduits and IAC Security Conduits are synonymous.

The IAC Security Conduit type (External, Intermediate, Internal) dictates what type of Security Zones can be connected. The IAC Security Conduit connectivity relationships are shown in Table 5-2 below:



| | | | | |
|---|---|---|---|---|
| External Zone | ↔ | IAC External Conduit | ↔ | IAC Intermediate Zone |
| IAC Internal Zone | ↔ | IAC Intermediate Conduit | ↔ | |
| | ↔ | IAC Internal Conduit | ↔ | IAC Internal Zone |

**Table 5-2: API 1164 IAC Security Conduit Connectivity Relationships**

Within the ONG pipeline industry IAC Security Conduits may use 3rd party communications transport network provider services. This includes, but is not limited to, GEO, MEO, or LEO satellite providers, POTS/PSTN telco networks, terrestrial leased line, wide-area-networks (WAN), metro-area-networks (MAN), MPLS, VPLS, and cellular modems. Regardless of the medium, these services provide varying levels of "black-box" network infrastructure. In this regard, the user of these services has little to no visibility of network management and access control procedures.

This document does not differentiate or subcategorize IAC Security Conduits between those that use third-party network infrastructure and those that use company owned network infrastructure. Both are considered external IAC transport services when the management of those network segments and services are not in the purview of IAC personnel. This document does, however, include additional requirements relative to the integrity of IAC networks, IAC baseline configurations, and IAC network and communication protections for IAC Security Conduits that use external IAC transport services.

### 5.4.1.5 IAC Zone and Conduit Example Implementation

The below diagram provides a visual example of an implementation of IAC Security Zones and IAC Security Conduits. The diagram is for explanatory and for reference purposes only.

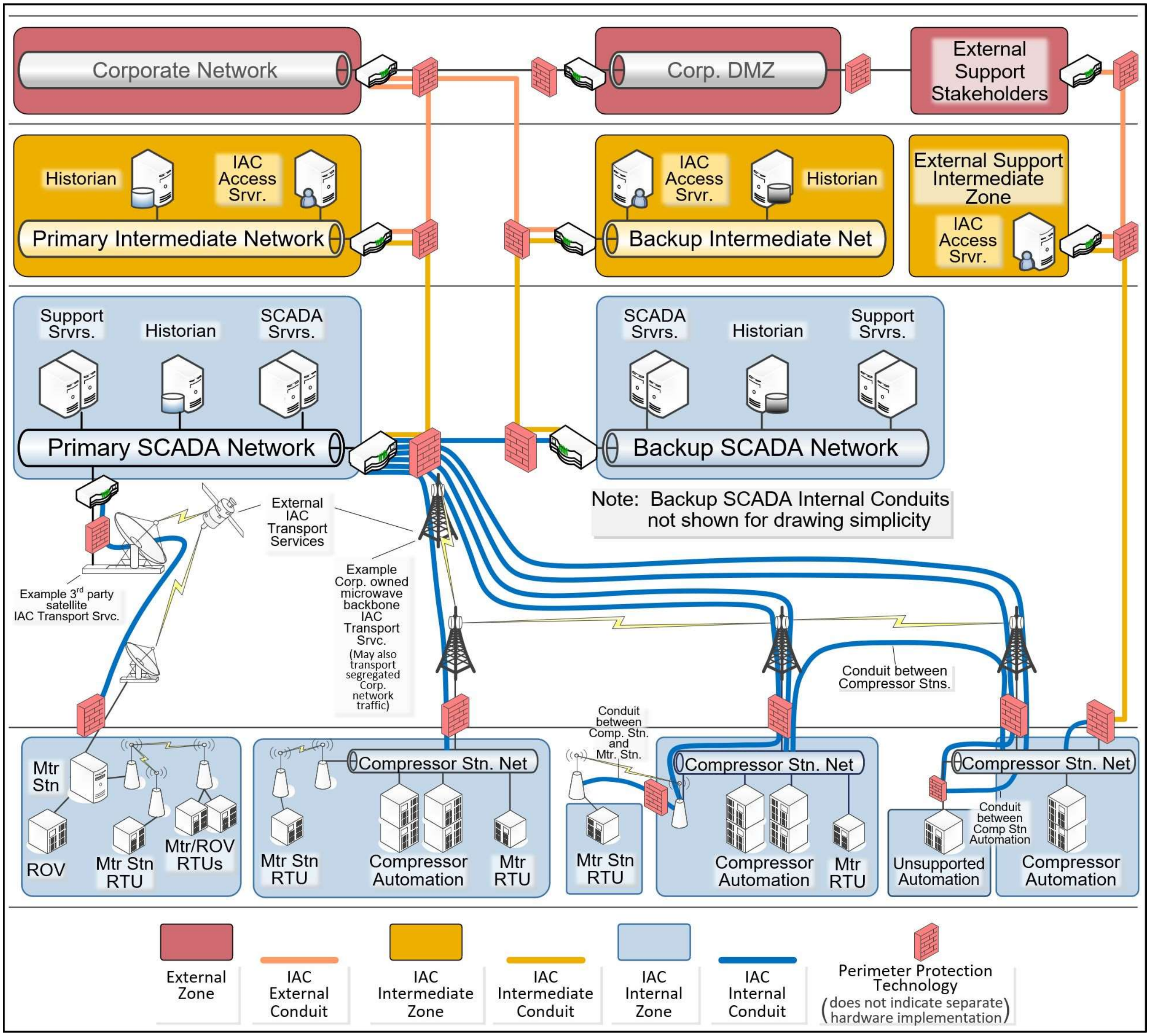


**Figure 5-5: Example API 1164 IAC Security Zone and Conduit Implementation**

#### 5.4.1.6 IAC Security Zoning Overview

This standard gives complete autonomy to its implementors in defining the boundaries of IAC Security Zones. This flexibility allows them to meet the requirements of a virtually limitless number of company specific considerations, architectures, and scenarios.

The justification for this flexibility is that the reason why an asset is included within a given IAC Security zone is not important. What is required is that the API 1164 Profile selected for the Security zone is based on the impact severity rating of the entire IAC Security Zone. This selected Profile is then applicable to all IAC Cyber Assets within the zone, regardless of an individual IAC Cyber Asset's impact rating. That is, an IAC Cyber Asset that would have selected the Baseline Profile based on its isolated impact rating must have its Profile selected based on the impact rating of the entire zone it belongs to, which could be higher. This enforces the highest-level protection across all IAC Cyber assets within the same zone to minimize a potential compromise of a lower impact IAC Cyber Asset putting at risk an IAC Cyber Asset with a potential higher impact to business objectives.

#### 5.4.1.7 IAC Security Zone Partitioning

The organization establishes zones and conduits by grouping IAC Cyber Assets. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

System inventory, architecture diagrams, network diagrams and data flows can be used to determine and illustrate the IAC assets that are considered for zone segmentation.

##### 5.4.1.7.1 Inventory Steps

1. Identify Cyber Asset inventory.
2. Identify functionality of assets including communications, monitoring, command and control and safety devices.
3. Disregard any cyber asset that is not used in the IAC resulting in the IAC cyber asset inventory.

NOTE External Zones and management of cyber assets that are not within an IAC Segregated Environment boundary are outside the scope of this standard.

4. Identify all Intra-company communications.
5. Identify all Inter-company communications.

##### 5.4.1.7.2 IAC Zone and Conduit Segmentation Rules

Organizations can create zones as they choose. IAC zone segmentation shall follow these rules:

1. All IAC Assets within an IAC Security zone must be on the same network segment or be able to be managed collectively as if on a single network segment.
2. All IAC Cyber Assets shall be a member of an IAC Segregated Environment and inherit the API 1164 Profile of the IAC Security Zone or IAC Security Conduit to which it belongs.
3. An IAC Segregated Environment only contains IAC Cyber Assets. The inclusion of any Cyber Asset into an IAC Segregated Environment, by definition, makes it an IAC Cyber Asset governed by the rules of the IAC Security Zone or IAC Security Conduit to which it belongs (e.g. including a printer within the IAC Security Zone boundary makes the printer and IAC Cyber Asset).
4. An IAC Security Zone cannot be contained within an External Zone (e.g. a subnet or VLAN within an enterprise network space).
5. All communication connections with IAC Cyber Assets within an IAC Security Zone shall be from other IAC Cyber Assets within the security zone or by an IAC Security Conduit interconnecting Security Zones.
6. An IAC Security Zone shall be connected to another Security zone only through IAC Security Conduit.
7. Production IAC Security Zones must be separate from IAC Security Zones used for development and testing.
8. Communications between IAC Cyber Assets and an External Zone must only occur from an IAC Intermediate Zone traversing an IAC Intermediate Conduit. (External ←→ Intermediate).

9. IAC Cyber Assets that provide data or services to an External Zone or receive data or services from an External Zone must only do so through IAC Intermediate Conduit connected to an IAC Intermediate Zone (External ←→ Intermediate ←→ IAC Internal).

#### 5.4.1.7.3 IAC Zone Segmentation Guidelines

Guidelines on how to create effective IAC Security Zones are listed below:

1. Group assets which contribute to a common function, location, or system.
2. Assets which have separate functions, locations, or systems can be grouped together into a common zone.
3. Wireless IAC Cyber Assets should be segregated into separate zones from IAC Security Zones containing wired IAC Cyber Assets.

NOTE Wireless includes wi-fi and other routable protocols which use radio frequency methods as a means of communications, not physical wires.

4. IAC Cyber Assets that can establish temporary zone conduit connections to an IAC Security zone should be segregated into a separate zone or zones from IAC Cyber Assets that are intended to establish permanent zone conduit connections.
5. Not all assets within a zone need to directly communicate with each other.

### 5.4.2 IAC Security Zone and Security Conduit Impact Assessment

Impact assessments are used to determine which API 1164 Security Profile is to be selected for IAC Security Zones and IAC Security Conduits. Zone impact assessments only apply to IAC Security Zones and not External Zones. Although an IAC External Conduit connects to an External Zone the impact from this conduit type is still in scope because the conduit also connected to an IAC Intermediate Zone, which is part of the IAC Cyber Environment.

Even though both IAC Security Zones and IAC Security Conduits are assessed for impact to the business objectives the Security Profile selection process is slightly different between the two. This is detailed below.

#### 5.4.2.1 IAC Security Zone Impact Assessment Rules

Zone impact assessments only apply to IAC Security Zones and not External Zones. Based on the shared security requirements of any given IAC Security Zone it should be assumed that a threat source may theoretically obtain a sufficient level of lateral movement within the IAC Security Zone to exploit a shared vulnerability intentionally or accidentally throughout the zone.

All IAC Cyber Assets within the boundaries of the IAC Security Zone are included in the collective impact severity calculation of the entire zone, not each IAC Cyber Asset impact severity calculated separately and individually. The process is to determine the impact severity of the IAC Security Zone using the Impact severity rating for all business objectives.

Organizations shall designate IAC Security Zones as having impact ratings. IAC Security Zone impact rating designation shall follow these rules:

1. An impact assessment shall be performed on the entire IAC Security Zone, not on individual assets
2. An IAC Security Zone's impact rating shall not be less than the highest impact rating of any IAC Cyber Asset it contains

   EXAMPLE: If for a given IAC Security Zone the business objectives of Reputation, Operations, Environment and Health/Safety are all at an Impact Severity of 1 but the Property business objective is an Impact Severity rating of 2, then the entire zone is considered to have an Impact Severity of 2. The zone would then be classified as an Enhanced Profile IAC Security Zone and the P2 security requirements will apply to all IAC Cyber Assets within the zone.

It is possible, and likely, that an IAC Security Zone can have a higher impact rating than the highest impact rating of any IAC Cyber Asset it contains.

#### 5.4.2.2 IAC Security Conduit Impact Assessment Rules

Since an IAC Security Conduit provides a connection between two Security Zones the conduit is assessed on the impact to business objectives from the conduit itself and the impact of the IAC Security Zones to which it connects.

Organizations shall designate IAC Security Conduits as having impact ratings. IAC zone impact rating designation shall follow these rules:

1. An impact assessment shall be performed on the entire IAC Security Conduit, not on individual assets
2. An IAC Security Conduit's impact rating shall not be less than the highest impact rating of any IAC Cyber Asset it contains

   EXAMPLE: If for a given IAC Security Conduit the business objective's Impact Severity of 1 but one of the two IAC Security Conduit's Business Objective Impact Severity rating is a 2, then the IAC Security Conduit is considered to have an Impact Severity of 2. The conduit would then be classified as an Enhanced Profile IAC Security Conduit and the P2 security requirements will apply to all IAC Cyber Assets within the conduit.

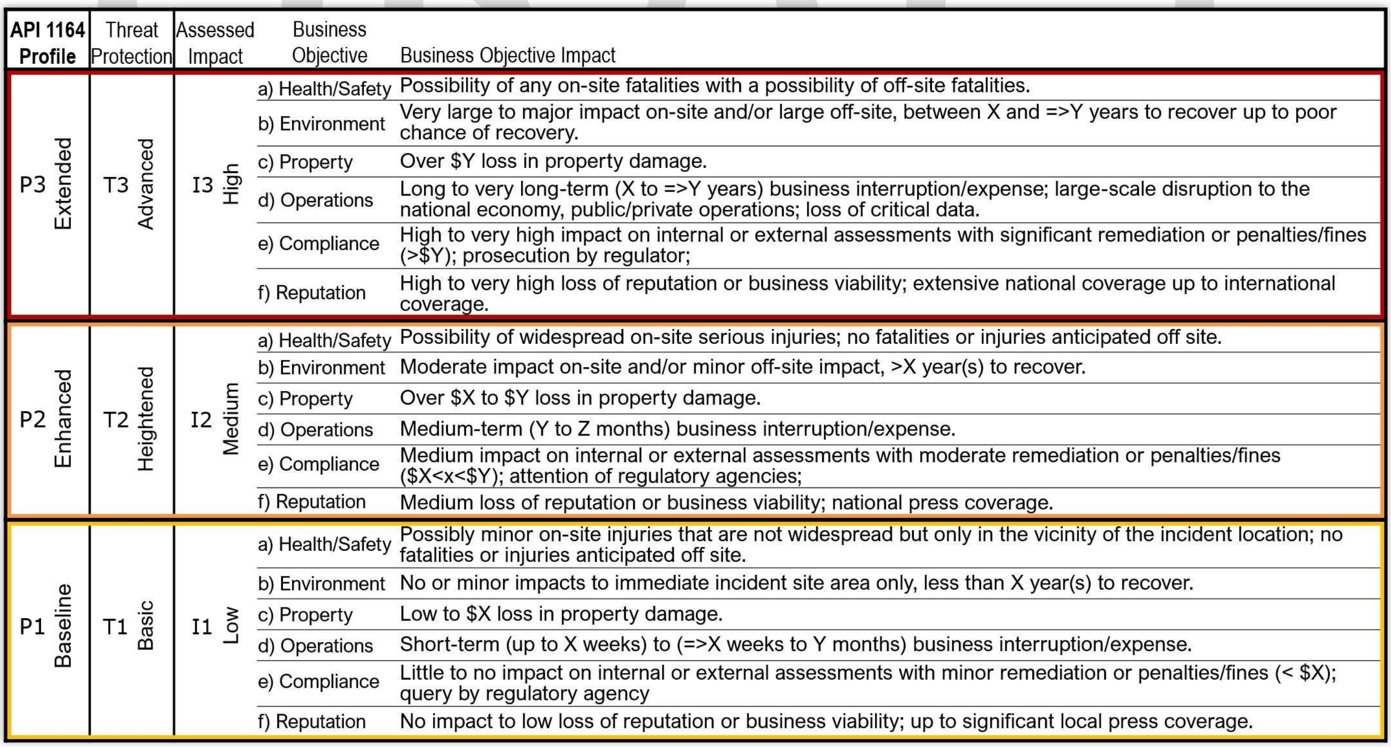
IAC Security Conduits can have a higher impact rating than either of the two IAC Security Zones to which it connects.

### 5.4.3 Security Zone and Conduit Profile Selection Process

Resource constraints dictate that it is not feasible to apply the most stringent and rigorous best practices to all IAC Cyber Assets and environments without regard to the risk they impose on the organization.

API 1164 focuses on assessing and classifying the potential impact to the organizational objectives by the compromise of an IAC Security Zone or IAC Security Conduit. These impact ratings have been aligned to API 1164 IAC Profiles. As previously detailed, these API 1164 Profiles were developed using threat protection objectives with increasing threat sophistication and motivation (see Section 4.3 IAC Cybersecurity Profile - Threat Protection Objectives on page 10 above). The result is a scaled approach whereby the higher the impact to business objectives the higher the protection level is required against a more advanced threat. This classification process categorizes an IAC Security Zone to apply an appropriate level of security to achieve a desired level of assurance based on the potential impact.

Table 5-3 below is to be used to determine which API 1164 Profile is required for an IAC Segregated Environment.



| API 1164 Profile | Threat Protection | Assessed Impact | Business Objective | Business Objective Impact |
|---|---|---|---|---|
| P3 Extended | T3 Advanced | I3 High | a) Health/Safety | Possibility of any on-site fatalities with a possibility of off-site fatalities. |
| | | | b) Environment | Very large to major impact on-site and/or large off-site, between X and =>Y years to recover up to poor chance of recovery. |
| | | | c) Property | Over $Y loss in property damage. |
| | | | d) Operations | Long to very long-term (X to =>Y years) business interruption/expense; large-scale disruption to the national economy, public/private operations; loss of critical data. |
| | | | e) Compliance | High to very high impact on internal or external assessments with significant remediation or penalties/fines (>$Y); prosecution by regulator; |
| | | | f) Reputation | High to very high loss of reputation or business viability; extensive national coverage up to international coverage. |
| P2 Enhanced | T2 Heightened | I2 Medium | a) Health/Safety | Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off site. |
| | | | b) Environment | Moderate impact on-site and/or minor off-site impact, >X year(s) to recover. |
| | | | c) Property | Over $X to $Y loss in property damage. |
| | | | d) Operations | Medium-term (Y to Z months) business interruption/expense. |
| | | | e) Compliance | Medium impact on internal or external assessments with moderate remediation or penalties/fines ($X<x<$Y); attention of regulatory agencies; |
| | | | f) Reputation | Medium loss of reputation or business viability; national press coverage. |
| P1 Baseline | T1 Basic | I1 Low | a) Health/Safety | Possibly minor on-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities or injuries anticipated off site. |
| | | | b) Environment | No or minor impacts to immediate incident site area only, less than X year(s) to recover. |
| | | | c) Property | Low to $X loss in property damage. |
| | | | d) Operations | Short-term (up to X weeks) to (=>X weeks to Y months) business interruption/expense. |
| | | | e) Compliance | Little to no impact on internal or external assessments with minor remediation or penalties/fines (< $X); query by regulatory agency |
| | | | f) Reputation | No impact to low loss of reputation or business viability; up to significant local press coverage. |

**Table 5-3: API 1164 IAC Business Objective Impact Classification Matrix**

Use the following steps to perform IAC Security Zone Impact Assessments:

1. Using the values appropriate for your organization update the table's variables.

NOTE These values are often obtained from organization authoritative sources familiar with risk and business financial thresholds.

2. Perform a detailed cybersecurity impact assessment for each zone to determine consequences and impacts.
3. Starting at the top of the matrix select the profile with the worst case (i.e. highest applicable) IAC Security Zone Impact using the consequence(s) and impact(s) determined during the impact assessment.
4. The resulting 1164 Profile is selected for all IAC Cyber Assets in the IAC Security Zone being classified.
5. Repeat steps 2 – 4 until all IAC Security Zones are categorized.

Use the following steps to perform the 1164 IAC Security Zone Conduit Impact Assessments:

1. Using the values previously derived from IAC Security Zone Impact Assessments in Step 1 above, perform a detailed cybersecurity impact assessment for each IAC Security Conduit to determine consequences and impacts.
2. Starting at the top matrix select the profile with the worst case (i.e. highest applicable) IAC Security Conduit Impact using the consequence(s) and impact(s) determined during the impact assessment.
3. If the resulting 1164 Profile selected is less than any 1164 Profile selected for all IAC Security Zones to which the IAC Security Conduit connects, the highest shall be selected for the IAC Security Conduit.
4. The resulting 1164 Profile is selected for all IAC Cyber Assets in the IAC Security Conduit being classified.
5. Repeat steps 1 – 4 until all IAC Security Conduits are categorized.

The organization then customizes the selected Security Profiles for each IAC Security Zone and IAC Security Conduit using its risk assessment process prior to implementation.

## 5.5 Customizing Selected Profile Requirements

The IAC Cybersecurity Program is based on the assessment of impact to business objectives from IAC Security Zones and IAC Security Conduits, and the selection of security requirements based on that impact. Given a virtually limitless number of company specific considerations, architectures and scenarios, this standard allows for the customization of the profile's requirements.

The tailoring of requirements for an IAC Segregated Environment can be influenced by any company specific unique risk limiting factors, including but not limited to, an organization's risk tolerance driven by its business or operating models, or the identification and consideration of additional existing mitigating controls or mitigating circumstances unique to the implementor's environment, architecture, or other unique risk limiting scenarios. The customization process may result in downgrading a requirement (i.e. implementation of a corresponding requirement from a lesser profile), modifying the requirement to fit the unique situation, or the elimination of the requirement entirely.

The customization process is not applied to the impact designated profile resulting in the downgrading of the profile for an IAC Segregated Environment in its entirety to a lower profile. It is only applied to each individual requirement within a profile. If all requirements of a profile are downgraded through the customization process for a given IAC Security Zone or Conduit the result is the risk justified implementation of lower profile requirements for a higher impact profile. The profile identified by the impact assessment never changes but the resulting requirements for that profile may represent a lower impact profile when all requirements are tailored in that regard.

This customization process uses the organization's risk management process and allows the organization to make risk-based decisions regarding the applicability of security requirements. Customization is a prerequisite to cybersecurity requirement implementation. The result of the customization process is a risk-appropriate list of IAC cybersecurity requirements for each IC Security Zone or Conduit that aligns to the organization's operating environment, business needs, and risk tolerance.

Customization activities should be well documented to help approving authorities make credible, risk-based decisions and avoid selection/deselection based on operational convenience. As environments and personnel change, the customization process artifacts provide historical context for the assumptions, constraints, and rationale used for those risk-based decisions. This historical perspective should be used when any reassessment is required.

The outcomes of the customization process should result in detailed risk assessments and actionable mitigations (controls) that are authorized by accountable personnel within the organization. The customized set of profile requirements and the supporting risk assessment artifacts are used to update the IAC Cybersecurity Plan as the baseline configuration to be implemented and operationalized as the customized IAC Cybersecurity Program.

# 6 ONG IAC Cybersecurity Profile Requirements - Identify (ID)

The Identify Function develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The target profiles outcome Categories and Subcategories within this Function are detailed below.

## 6.1 Governance (ID.GV)

The objective is to employ an organization-wide formal IAC cybersecurity management program to address the cybersecurity aspects of its IAC Cyber Environments. The implementation of the IAC program requires the establishment of formal IAC Security Program documentation in the form of policies, procedures, processes, and operational and procedural controls. These documents detail the organization's cybersecurity regulatory, legal, risk, and operational requirements, how the requirements are satisfied, and how they are managed and monitored in the form of specific people, processes, and technology.

A governance model can then be used to measure the performance of the actual execution of the program against the requirements, deliverables, and outcomes set forth in its formal documentation.

It is critical that the IAC Cybersecurity Program documents are collaboratively developed, officially approved, and conspicuously published. Policies are approved by senior leadership, which authorizes the resulting program implementation. It is imperative the IAC Security Program documents are well understood through formal training and awareness processes, roles and responsibilities for the management and operation of the program are appropriately assigned and communicated use formal training, and the operation of the program and the governance of it informs management of its IAC cybersecurity risk.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

### 6.1.1 Baseline Profile Requirements

1) A formal IAC Cybersecurity Policy exists that specifies the requirements for and authorizes the implementation of a risk-based IAC Cybersecurity Program.
2) The IAC Cybersecurity Policy requires that the IAC Cybersecurity Program be developed, implemented, and operated as specified in a documented IAC Cybersecurity Plan.
3) The requirements of IAC Cybersecurity Policy are communicated to and agreed by relevant IAC stakeholders prior to accessing any IAC Cyber Environment.
4) The IAC Cybersecurity Policy is approved by senior leadership accountable for the IAC Program.
5) The IAC Cybersecurity Policy is reviewed at organizationally defined frequency and updated as appropriate no less often than every 36 months.

### 6.1.2 Enhanced Profile Requirements

6) The IAC Cybersecurity Policy is reviewed and updated as appropriate no less often than every 12 months by any organization that has one or more IAC Segregated Environments classified with an API 1164 Impact Rating of I2-Medium or higher.

### 6.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.1.4 ID.GV-1 – IAC Cybersecurity Plan

The IAC Cybersecurity Plan is one or more formal documents that specify all the requirements and outcomes of an IAC Cybersecurity Program. It specifies all foundational building elements, including the procedures, processes, roles and responsibilities of stakeholders, and procedural and technical controls required to operationalize a risk-appropriate IAC Cybersecurity Program. It is scoped for IAC Cyber Environments, which addresses specific IAC cybersecurity and IAC operational requirements, constraints, and considerations when defining an IAC Cybersecurity Program.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 6.1.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that governance processes exist that inform the management of IAC cybersecurity risk of the organization's regulatory, legal, environmental, and operational risk.
2) The IAC Cybersecurity Plan requires that the IAC Cybersecurity Program be measured for performance.
3) The IAC Cybersecurity Plan requires that any IAC Cybersecurity Program performance deficiencies be addressed.
4) The IAC Cybersecurity Plan requires that the IAC Cybersecurity Policy and IAC Cybersecurity Plan be updated to reflect any IAC Cybersecurity Program performance corrections.
5) The IAC Cybersecurity Plan is reviewed at an organizationally defined frequency and updated as appropriate no less often than every 36 months.

#### 6.1.4.2 Enhanced Profile Requirements

6) The IAC Cybersecurity Plan is reviewed and updated as appropriate no less often than every 24 months by any organization that has one or more IAC Cyber Environments with an impact classification higher than I1.

#### 6.1.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.1.4.4 Supplemental Guidance

a) The IAC Cybersecurity Policy should specify consequences for violation of policy, including, but not limited to, potential disciplinary actions in accordance with Company defined policy compliance requirements.
b) The IAC Cybersecurity Plan should be reviewed and assessed in alignment with overall management system requirements of the organization (e.g. relevant requirements in API Recommended Practice 1173 – Pipeline Safety Management Systems). This would include management review, establishing performance indicators and tracking performance of the program to inform updates to the IAC Cybersecurity Program.

#### 6.1.4.5 IIoT Cautions and Supplemental Guidance

c) If IIoT deployment becomes pervasive, identifying relevant IIoT stakeholders may impose communication/training challenges.

### 6.1.5 ID.GV-2 – ICS Cybersecurity Roles and Responsibilities Coordination

The organization aligns IAC cybersecurity roles and responsibilities with internal and external partners. Identification of individual contributors and stakeholders, their responsibilities and commitment requirements are paramount to an effective cybersecurity program. In the event of a cybersecurity incident a defined and understood responsibility matrix is the key to a well-organized response.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 6.1.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires the identification of IAC cybersecurity stakeholder roles, including internal and external partners.
2) The IAC Cybersecurity Plan requires that IAC cybersecurity be coordinated between stakeholders.
3) The IAC Cybersecurity Plan requires that the roles and responsibilities of the ICS Cybersecurity Program be coordinated between any existing company functions and with IAC operations.

   See associated requirements in Section 6.6.4 ID.AM-6 – Cybersecurity Roles and Responsibilities on page 42.
4) The IAC Cybersecurity Plan requires the documentation of where the responsibility and accountability for the design, implementation, management, administration, or operations of IAC cybersecurity transitions between intra-organizational or inter-organizational boundaries.

5) The IAC Cybersecurity Plan requires that any IAC cybersecurity responsibility and accountability reassignment be formally agreed to by all involved stakeholders and documented.
6) The IAC Cybersecurity Plan requires that management-of-change processes, at minimum, consult and inform all associated stakeholders on any modifications impacting an IAC cybersecurity responsibility and accountability transition point. (e.g. Changes to firewall rules are communicated to the stakeholders of the IAC Security Conduits and the IAC Security Zones connected to or associated with the firewall).

#### 6.1.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.1.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.1.5.4 Supplemental Guidance

a) When addressing ICS cybersecurity roles and responsibilities coordination in the IAC Cybersecurity Plan, organizations should consider referencing Figure 5-2: IAC Cybersecurity Plan Development Participation for a list of potential stakeholders that may require some level of coordination.

#### 6.1.5.5 Natural Gas Transmission Pipeline Supplemental Guidance

b) Special consideration should be given to ICS cybersecurity roles and responsibilities coordination regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 6.1.6 ID.GV-3 – ICS Cybersecurity Legal and regulatory requirements

The organization understands its legal, regulatory, and contractual requirements. These requirements can impact an organization's business objectives. Compliance with these requirements helps organizations avoid breaches of legal, regulatory, or contractual obligations related to IAC cybersecurity.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 6.1.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that sources of legal and regulatory requirements applicable to or impacting IAC cybersecurity (e.g. contracts, local, state, tribal, federal, international laws, and regulations) are cataloged.
2) The IAC Cybersecurity Plan requires that sources of applicable legal and regulatory cybersecurity requirements (e.g. contracts, local, state, tribal, federal, international laws, and regulations) are cataloged.
3) The IAC Cybersecurity Plan requires that legal and regulatory requirements be included in risk management decisions.
4) The IAC Cybersecurity Plan requires that legal and regulatory cybersecurity requirements be clearly communicated to stakeholders.

#### 6.1.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.1.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.1.6.4 Supplemental

a) Organizations should consider formal training is satisfactorily completed at a risk-appropriate frequency on applicable legal and regulatory cybersecurity requirements based on IAC user role.
b) Organizations should consider explicitly mapping applicable cybersecurity controls to legal and regulatory requirements.

### 6.1.7 ID.GV-4 – ICS Cybersecurity Governance and Risk Management

Governance and risk management strategies identify the risk tolerance for an organization, what methodologies will be used in assessing risk, strategies to mitigate risk, and a means to periodically evaluate risk in accordance with the organization's risk tolerance.

A well-formed governance and risk management strategy will aid an organization in facilitating a consistent, organization-wide approach in mitigation or acceptance of risk.

Risk management is a fundamental principle of cybersecurity. Managing cybersecurity risk allows an organization to adhere to accepted risk levels for its business objectives.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 6.1.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires the governance and management of IAC cybersecurity risks.
2) The IAC Cybersecurity Plan requires that IAC cybersecurity governance and risk management consider enterprise cybersecurity governance and risk management.

#### 6.1.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.1.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

## 6.2 Risk Management Strategy (ID.RM)

Risk Management Program is the fundamental cybersecurity program capability. It is a collection of people, processes, and optional technology to systematically address risk, including cybersecurity risk, to organizational objectives (including mission, functions, image, reputation), organizational assets, individuals, and other organizations. See Section 5.2 IAC Cybersecurity Plan - Risk Management on page 15 above.

The foundation of a Risk Management Program is the Risk Strategy. It is a structured framing that addresses how organizations intend to assess, respond to, and monitor risk. The risk management strategy is a formal declaration of the organization's priorities (e.g. importance of missions/business functions and trade-offs between varying types of risk), constraints on the risk assessment, response and monitoring alternatives, risk tolerances (e.g. levels and types of risk, and degree of risk uncertainty that are acceptable), and assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time. The risk management strategy is explicit, transparent, and used to support operational risk decisions.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

### 6.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires that an IAC Risk Management Program exists as part of the overall IAC Cybersecurity Program to manage IAC cybersecurity risk to availability, integrity, and information security of the organization's IAC Cyber Environment(s).
2) The IAC Cybersecurity Policy requires that a formal IAC Risk Management Strategy exists as part of the overall IAC Risk Management Program, which specifies the organization's IAC cyber risk priorities, constraints, tolerances, and assumptions to support operational risk decisions.
3) The IAC Cybersecurity Plan requires that identified IAC cybersecurity risk is only communicated to risk appropriate stakeholders.

### 6.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.2.4 Supplemental Guidance

a) All factors used in a risk calculation, including the likelihood factors of vulnerabilities and threats along with the impact factors and the resulting risk determination should be protected and only communicated to those with a legitimate business need to know. Those with a need-to know would be considered risk appropriate to receive such information.

### 6.2.5 ID.RM-1 – Risk Management Program

Managing cybersecurity risk is a complex activity that requires the involvement of the entire organization, including senior leaders/executives, mid-level leaders, and individuals operating the control systems supporting the organization's missions/business functions. A risk management process is comprehensive and requires the organization to: 1) frame risk (i.e. context for risk-based decisions); 2) assess risk (see Section 6.5 below); 3) respond to risk once determined (see Section 6.5.9 below); and 4) monitor risk on an ongoing basis. Risk management is carried out as a holistic, organization wide activity that addresses risk from the strategic level to the tactical level. It ensures that risk-based decisions are integrated into every aspect of the organization. Risk management processes must be agreed to by organizational stakeholders and actively managed.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 6.2.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the enterprise risk management strategy be considered when defining IAC Cybersecurity Risk Management Strategy.
2) The IAC Cybersecurity Plan requires that the operations risk management strategy be considered when defining IAC Cybersecurity Risk Management Strategy.

#### 6.2.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.2.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.2.6 ID.RM-2 – Risk Tolerance

A risk management strategy is an explicit declaration of the organization's risk priorities, constraints on the risk assessment, response and monitoring alternatives, risk tolerances (e.g. levels and types of risk, and degree of risk uncertainty that are acceptable), and assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time. An organization's risk tolerance is determined and clearly expressed within the Risk Strategy.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (4); | **P3:** (1); (2); (5); |

#### 6.2.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Risk Management Strategy considers enterprise risk tolerance when documenting IAC risk tolerance.
2) The IAC Cybersecurity Plan requires that the IAC risk tolerance be approved by organizationally defined stakeholders.
3) The IAC Cybersecurity Plan requires that the IAC Risk Management Strategy specifies risk tolerance for Baseline Profile IAC Segregated Environments.

#### 6.2.6.2 Enhanced Profile Requirements

4) The IAC Cybersecurity Plan requires that the IAC Risk Management Strategy specify risk tolerance for Enhanced Profile IAC Segregated Environments.

#### 6.2.6.3 Extended Profile Requirements

5) The IAC Cybersecurity Plan requires that the IAC Risk Management Strategy specify risk tolerance for Extended Profile IAC Segregated Environments.

### 6.2.7 ID.RM-3 – Critical Infrastructure and Sector Specific Risk Tolerance

The organization's place in critical infrastructure and its industry sector should be identified and clearly communicated. The objective of the Critical Infrastructure and Sector Specific Risk Tolerance activities is to ensure the organizational roles in these contexts are considered during risk analysis in the organization's determination of its risk tolerance and resulting risk responses.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 6.2.7.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 6.2.7.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that risk management processes document the organization’s role in the critical infrastructure and other sector specific risk in the IAC Risk Management Strategy document.
2) The IAC Cybersecurity Plan requires that the organization's role in the critical infrastructure and other sector specific risk is incorporated into the organization's risk tolerance posture.
3) The IAC Cybersecurity Plan requires that the organization’s role in the critical infrastructure and other sector specific risk is considered in risk management decisions including, but not limited to, risk assessment (e.g. likelihood and impact calculations), rating risk (e.g. risk criticality rating), and risk response actions and prioritization.
4) The IAC Cybersecurity Plan requires that the organization’s role in the critical infrastructure and other sector specific risk is considered in decisions regarding the definition of roles and assignment of responsibilities.
5) The IAC Cybersecurity Plan requires that IAC cybersecurity awareness training clearly communicates and educates on the organization’s role in the critical infrastructure and other sector specific risk.

#### 6.2.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.2.7.4 Supplemental Guidance

a) The role in critical infrastructure and other sector specific factors should be considered when assessing or managing the risk of IAC Cyber Environments.

## 6.3 Business Environment (ID BE)

Cybersecurity roles, responsibilities, and risk management decisions depend on the Business Environment that an organization operates in. The objective of understanding the Business Environment as it relates to cybersecurity is to prioritize and communicate the protection strategy, accounting for the organization’s mission, objectives, critical services, and relation to the critical infrastructure of the sector in which the organization operates.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); | **P3:** (1); |

### 6.3.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

### 6.3.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Policy requires that the IAC Risk Management Strategy document the organization’s role in the critical infrastructure essential products and services supply chain, both upstream critical infrastructure suppliers and downstream critical infrastructure customers.

NOTE See Section 6.2 Risk Management Strategy (ID.RM) on page 28 above).

### 6.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.3.4 ID.BE-1 – Critical Infrastructure Supply Chain Role

To ensure the organization understands the entirety of the potential risk associated with its operations, it is necessary that the organization’s role in the critical infrastructure supply chain is identified and communicated. The objective of the Critical Infrastructure Supply Chain Role activities is to ensure the organizational roles within the supply chain are identified and considered during risk analysis and the organization’s determination of risk tolerance and risk responses.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 6.3.4.1 Baseline Profile Requirements

None.

#### 6.3.4.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that the organization's role in the critical infrastructure supply chain influences the organization's risk tolerance posture.
2) The IAC Cybersecurity Plan requires that the organization’s role in the critical infrastructure supply chain is included in risk management decisions including, but not limited to, risk assessment (e.g. likelihood and impact calculations), rating risk (e.g. risk criticality rating), and risk response actions and prioritization.
3) The IAC Cybersecurity Plan requires that the organization’s role in the critical infrastructure supply chain is included in decisions regarding the definition of roles and assignment of responsibilities.
4) The IAC Cybersecurity Plan requires that IAC cybersecurity awareness training clearly communicates and educates on the organization’s role in the critical infrastructure supply chain.

#### 6.3.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.3.4.4 Supplemental Guidance

a) The impact of IAC essential function disruptions and outages should be influenced by their role in critical infrastructure supply chain.

### 6.3.5 ID.BE-2 – Critical Infrastructure and Industry Sector Roles

The role of an organization in providing for, and supporting, critical infrastructure and industry sectors should be defined, understood, and communicated. This is important to meet the objective of developing protection strategies based on the prioritization of critical assets and resources.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 6.3.5.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 6.3.5.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Risk Management Strategy documents the organization’s role in the critical infrastructure and other sector specific risk.
2) The IAC Cybersecurity Plan requires that the organization's role in the critical infrastructure and other sector specific risk is incorporated into the organization's risk tolerance posture and risk responses.
3) The IAC Cybersecurity Plan requires that the organization’s role in the critical infrastructure and other sector specific risk is included in risk management decisions including, but not limited to, risk assessment (e.g. likelihood and impact calculations), rating risk (e.g. risk criticality rating), and risk response actions and prioritization.

#### 6.3.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.3.5.4 Supplemental Guidance

a) An IAC Cyber Asset’s role in critical infrastructure should be considered during its IAC Security Zone or IAC Security Conduit impact assessment.

### 6.3.6 ID.BE-3 – Priorities of Mission, Objectives, and Activities

To protect against threats to organizations, assets, or critical infrastructure, data and information should be protected. Information protection expectations are derived from the mission and business needs defined by the organization, the processes selected to meet those needs, and the organizational risk management strategy. The objective is to identify core organizational missions supported by the system to appropriately prioritize the protection strategy.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

### 6.3.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the priorities of the organization's mission, objectives, and activities be included in decisions regarding the definition of roles and assignment of responsibilities.

NOTE See Section 6.6.4 ID.AM-6 – Cybersecurity Roles and Responsibilities on page 42 below.

2) The IAC Cybersecurity Plan requires that the priorities of the organization's mission, objectives, and activities are included in risk management decisions, including, but not limited to, risk assessment (e.g. impact calculations), risk calculation (e.g. criticality rating), and risk response actions and prioritization.

NOTE See Section 6.2 ID.RM-1 – Risk Management Program on page 29 above).

3) The IAC Cybersecurity Plan requires that the IAC cybersecurity training program clearly communicates and educates on the organization's mission, objectives, and activities priorities.

### 6.3.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.3.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.3.7 ID.BE-4 – Critical Services Delivery Dependencies

Understanding the dependencies of critical services helps prioritize the implementation of security measures to protect the availability, integrity, and data of the control systems' essential functions required for those critical services.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); | **P3:** (1); (2); |

### 6.3.7.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

### 6.3.7.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that essential functions required for the delivery of critical services are cataloged.

2) The IAC Cybersecurity Plan requires that essential functions required for the delivery of critical services are included in risk management decisions, including, but not limited to, risk assessment (e.g. impact calculations), risk calculation (e.g. criticality rating), and risk response actions and prioritization.

NOTE See Section 6.3 ID.BE-1 – Critical Infrastructure Supply Chain Role on page 30, above.

### 6.3.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.3.7.4 Supplemental Guidance

a) The impact of IAC essential function disruptions and outages should be influenced by their role in critical infrastructure.

### 6.3.8 ID.BE-5 – Critical Services Delivery Resiliency

Identifying the resiliency requirements for delivery of critical services is necessary to understand the security measures needed to protect the availability, integrity, and data of the control systems' essential functions required for those critical services.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

### 6.3.8.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 6.3.8.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that a risk-based IAC Critical Services Resiliency Plan exists to manage the resiliency posture of IAC essential functions required for critical service delivery.
2) The IAC Cybersecurity Plan requires that the IAC Critical Services Resiliency Plan identifies all operating states (e.g. normal, diminished operations, under duress/attack, stabilization/recovery, etc.) for IAC essential functions required for critical service delivery.
3) The IAC Cybersecurity Plan requires that the IAC Critical Services Resiliency Plan establishes consistent criteria for determining the tolerance for disruption of IAC essential functions.
4) The IAC Cybersecurity Plan requires that he IAC Critical Services Resiliency Plan defines risk-based resiliency requirements for all identified operating states for all IAC essential functions necessary for critical service delivery.

#### 6.3.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.3.8.4 Supplemental Guidance

a) The IAC Critical Services Resiliency Plan is not required to be a separate document but alternatively can be called out separately in the IAC Cybersecurity Plan.
b) The impact of IAC essential function disruptions and outages should be influenced by their role in critical infrastructure.
c) A key component for resiliency is developing, implementing, and testing appropriate contingency plans.

NOTE See Section 7.4.9 PR.IP-9 – Incident Response and Contingency Plans on page 70 below for additional contingency plan requirements.

## 6.4 Supply Chain Risk Management (ID.SC)

Managing potential risk introduced by the digital technology supply chain is foundational to safeguarding the essential functions of the control system domain. Selecting cybersecurity mature vendors and products through a formal supply chain risk assessment process is a fundamental risk management strategy element to building and maintaining a holistic security ecosystem. The risk management strategy establishes the organization’s priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated with managing supply chain risk. The objective is the organization establishes and implements the processes to identify, assess, and manage supply chain risks.

### 6.4.1 ID.SC-1 – IAC Supply Chain Risk Management

Establishing digital technology supply chain risk management is key to safeguarding the essential functions of the IAC Cyber Environment. The objective is to ensure supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 6.4.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Supply Chain Risk Management Program exists to address risk imposed by the supply chain on IAC essential functions.
2) The IAC Cybersecurity Plan requires that the Supply Chain Risk Management Program defines operational or procedural controls to manage risk associated with acquiring digital technology products and services used in or by the IAC Cyber Environment.
3) The IAC Cybersecurity Plan requires that the Supply Chain Risk Management Program be integrated with the overall IAC Risk Management Program.

#### 6.4.1.2 Enhanced Profile Requirements

4) The IAC Cybersecurity Plan requires that the IAC Supply Chain Risk Management Program specifies processes to include safeguards to protect against supply chain threats.

#### 6.4.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.4.1.4 Supplemental Guidance

a) The IAC Supply Chain Risk Management Program may be defined in a separate document or within the IAC Cybersecurity Plan itself as a separate section.

b) Standard cybersecurity procurement language should be developed and included in all contracts for purchase of digital technology products and services that specify minimum security requirements.

c) The organization should consider requiring IAC Cyber Assets and IAC Systems, which are used in or in support of IAC Segregated Environments with an API 1164 Impact Rating of I2-Medium or higher, be reviewed by independent assessors. The organization should consider requiring a security level assurance certification (e.g. ISASecure IEC 62443 Conformance Certification).

### 6.4.2 ID.SC-2 – IAC Supply Chain Risk Assessment

An IAC Supply Chain Risk Management process should include the categorization, prioritization, and assessment of suppliers and partners based on the level of reliance by IAC essential functions. The objective of the Supply Chain Risk Assessment process is to apply the appropriate level of scrutiny to vendor (product and services) selection based on the risk imposed by the supply chain on IAC essential functions.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8): |

#### 6.4.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the suppliers of IAC Cyber Assets listed within the asset inventory are identified.

#### 6.4.2.2 Enhanced Profile Requirements

2) The IAC Cybersecurity Plan requires that a supply chain risk assessment process be defined to identify, categorize, and prioritize cyber risk to the IAC Cyber Environment.

3) The IAC Cybersecurity Plan requires that the IAC supply chain risk assessment process include IAC Cyber Assets and Services performed on the IAC Cyber Environment or within the IAC Cyber Environment.

4) The IAC Cybersecurity Plan requires that consistent criteria be established to categorize and assess risk to the IAC Cyber Environment imposed by the IAC supply chain.

5) The IAC Cybersecurity Plan requires that the supply chain risk categorization includes impact to IAC essential functions.

6) The IAC Cybersecurity Plan requires that IAC supply chain risk be addressed in accordance with the IAC Risk Management Strategy.

7) The IAC Cybersecurity Plan requires that the IAC supply chain risk be reassessed periodically at an organizationally defined frequency.

#### 6.4.2.3 Extended Profile Requirements

8) The IAC Cybersecurity Plan requires that the IAC supply chain risk be reassessed no less often than 3 years and not to exceed 45 months.

#### 6.4.2.4 Supplemental Guidance

a) Standard cybersecurity procurement language should be developed and included in all contracts for purchase of cyber technology products and services that specify minimum security requirements.

b) Organizations should consider having an independent assessor review IAC Cyber Assets that are a member of an IAC Segregated Environment with an impact rating greater than I1-Low

c) Organizations may consider requiring security level assurance certification (e.g. ISASecure IEC 62443 Conformance Certification) IAC Cyber Assets that are a member of an IAC Segregated Environment with an impact rating of I3-High.

### 6.4.3 ID.SC-3 – Supply Chain Obligations

Including contractual requirements that products and services meet the objectives of the organization’s IAC Cybersecurity Program is foundational to supply chain risk management. The objective of Supply Chain Obligations is to help enforce those obligations beyond the vendors’ normal position of operating based on positive intent and in good faith.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

### 6.4.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC cybersecurity requirements be included in contracts with suppliers.
2) The IAC Cybersecurity Plan requires that IAC cybersecurity requirements be explicitly communicated to IAC technology supply chain vendors.

### 6.4.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.4.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.4.3.4 Supplemental Guidance

a) Standard cybersecurity procurement language should be developed and included in all contracts for purchase of IAC Cyber Assets and IAC Cyber Environment service, which specify minimum security requirements.

## 6.4.4 ID.SC-4 – Supply Chain Risk Management Compliance

Fundamental to any risk management process is reliance on a trust/verify model. Constant controls monitoring or automated verification is often neither practical nor achievable. The objective of Supply Chain Risk Management Compliance is to verify the cybersecurity obligations by assessing reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

### 6.4.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC cybersecurity requirement auditing, assessment, or validation method options, including frequency, are included in IAC supply chain procurement requirements.

### 6.4.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.4.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.4.4.4 Supplemental Guidance

a) The verification frequency of contractually obligated IAC cybersecurity requirements should be proportional to the impact rating of the IAC Segregated Environment for the IAC Cyber Asset or service under consideration.
b) When IAC Cyber Solutions are self-evaluated by manufacturers, suppliers, service providers, and system integrators, special consideration should be taken on the evaluation method and threshold criteria.

## 6.4.5 ID.SC-5 – Supply Chain Risk Management Incident Response

One facet of risk management planning includes informing the IAC supply chain vendors of the dependencies from the organization’s response and recovery requirements. The objective of Supply Chain Risk Management Incident Response is to include dependent supply chain resources in incident response plans and activities.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); (2); | **P3:** (1); (2); |

### 6.4.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that digital technology supply chain dependencies be considered in response and recovery plans.

#### 6.4.5.2 Enhanced Profile Requirements

2) The IAC Cybersecurity Plan requires that digital technology supply chain vendors be included when response and recovery plans are exercised.

#### 6.4.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.4.5.4 Supplemental Guidance

a) Based on the criticality of the cyber asset, IAC Cyber Asset or the IAC system the organization may consider contracting for service level agreement (SLA) based spares availability or service/system restoration timing.

b) Based on the impact from IAC essential function disruptions or outages, the organization may consider contracting for service level agreement (SLA) based IAC Cyber Asset spares availability or service/system restoration timing.

## 6.5 IAC Risk Assessment (ID.RA)

The purpose of the IAC risk assessment process is to identify 1) threats to operations, IAC Cyber Assets, or individuals; 2) vulnerabilities of IAC Cyber Assets 3) the consequences/impact (i.e. harm) to the organization that may occur given the potential for threats exploiting vulnerabilities; and 4) the likelihood that harm will occur. The result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring) such that the organization understands the cybersecurity risk to organizational operations (including mission, essential functions, or reputation), organizational assets, individuals, and the upstream and downstream supply chain ecosystem, including risk to critical infrastructure.

| | | |
|---|---|---|
| **P1** (1); (2); | **P2** (1); (2); | **P3** (1); (2); |

### 6.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy specifies, either directly or by reference to other company approved policy, the company's risk-appropriate responsible disclosure requirements for internally discovered vulnerabilities found in its IAC cyber technology supply chain solutions.

2) The IAC Cybersecurity Plan requires that management who is accountable for the safety, integrity and reliability of an IAC Segregated Environment shall review and approve the results of a risk assessment prior to any Risk Response activity being implemented in an IAC Segregated Environment. (See: Section 6.5.9 ID.RA-6 – Responding to Risk on page 41 below).

### 6.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.5.4 ID.RA-1 – Asset Vulnerability Identification

An effective cybersecurity risk management program recommends that an asset's level of protection be directly proportional to the impact caused by a cyber compromise of that asset. Identification of security control gap vulnerabilities, which are insufficient levels of protection, is a required first step in understanding the cybersecurity risk imposed by that asset.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); (17); (18); (19); (20); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); (17); (18); (19); (20); |

#### 6.5.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires the cataloging of identified vulnerabilities (IAC cyber vulnerability catalog) in all IAC Segregated Environments.

2) The IAC Cybersecurity Plan requires that consistent criteria be established to identify IAC vulnerabilities.

3) The IAC Cybersecurity Plan requires that applicable IAC vulnerabilities published, announced, or disclosed from vendors, researchers, and other sources are included in the IAC vulnerability catalog.

4) The IAC Cybersecurity Plan requires that the identification of vulnerabilities includes risk-appropriate internal IAC cybersecurity assessment activities (e.g. pen test, Red-team, Blue-team, internal audits, etc.).
5) The IAC Cybersecurity Plan requires that consistent criteria be established to assess and categorize (e.g. type, severity rating, etc.) identified IAC Segregated Environment vulnerabilities.
6) The IAC Cybersecurity Plan requires that the identification and categorization of vulnerabilities includes an assessment of the design effectiveness of IAC Segregated Environment technical security controls. (i.e. The technical security controls in place are designed sufficiently to achieve the control objectives).
7) The IAC Cybersecurity Plan requires that the assessment of design effectiveness of technical security controls includes the assessment of physical compensating controls needed or implemented.
8) The IAC Cybersecurity Plan requires that the identification and categorization of vulnerabilities includes an assessment of the operating effectiveness of IAC Segregated Environment technical security controls. (i.e. The technical security controls in place are operated to achieve the control objectives).
9) The IAC Cybersecurity Plan requires that the identification and categorization of vulnerabilities includes an assessment of the design effectiveness of IAC Segregated Environment procedural security controls. (i.e. The procedural security controls in place are designed sufficiently to achieve the control objectives).
10) The IAC Cybersecurity Plan requires that the assessment of design effectiveness of procedural security controls includes the assessment of physical compensating controls needed or implemented.
11) The IAC Cybersecurity Plan requires that the identification and categorization of vulnerabilities includes an assessment of the operating effectiveness of IAC Segregated Environment procedural controls. (i.e. The procedural security controls are operating as designed and the persons performing control activities have sufficient authority and competence to perform them effectively to achieve the control).
12) The IAC Cybersecurity Plan requires that the identification (e.g. name, tag, label, etc.), assessment results, and categorization attributes of the IAC vulnerabilities are included in the IAC vulnerabilities catalog.
13) The IAC Cybersecurity Plan requires that risk management processes identify risk to the IAC Cyber vulnerability catalog associated with unauthorized disclosure and modification.
14) The IAC Cybersecurity Plan requires that the IAC Cyber vulnerability catalog be classified and protected according to identified risk.
15) The IAC Cybersecurity Plan requires that IAC Stakeholders responsible for the IAC vulnerability cataloging are, at minimum, consulted and informed through formalized management-of-change processes on any modification that could impact the cybersecurity of the IAC Cyber Environment.
16) The IAC Cybersecurity Plan requires that the identification, assessment, and cataloging of IAC vulnerabilities recurs periodically, based on company defined risk criteria including, at minimum, the impact rating of the IAC Security Zones and IAC Security Conduits. (IAC Segregated Environment components).

### 6.5.4.2 Enhanced Profile Requirements

17) The IAC Cybersecurity Plan requires that the design effectiveness of IAC Segregated Environment cybersecurity controls be reassessed no less often than every 3 years not to exceed 45 months.
18) The IAC Cybersecurity Plan requires that the operating effectiveness of IAC Segregated Environment cybersecurity controls be reassessed no less often than every 3 years not to exceed 45 months.
19) The IAC Cybersecurity Plan requires that the design effectiveness of IAC cybersecurity controls be assessed within 12 months of a newly identified IAC Segregated Environment or a significant modification thereto.
20) The IAC Cybersecurity Plan requires that the operating effectiveness of cybersecurity controls be assessed within 18 months of a newly identified IAC Segregated Environment or a significant modification thereto.

### 6.5.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.5.4.4 Supplemental Guidance

a) A good reference for the consistent risk assessment categorization criteria is the Technical Report: A Taxonomy of Operational Cyber Security Risks Version 2, Software Engineering Institute CMU/SEI-2014-TN-006, copyright 2014 Carnegie Mellon University.

b) A diverse set of sources and activities can be used to identify types of asset vulnerabilities. Some of these methods that may be considered are identification of system/architectural flaws, analysis of system documentation, security directives, tabletop exercises, notification of discovered vulnerabilities, code analysis, software version checking.

c) Conflicts of interest between the control assessment activities and the control operation activities should be avoided following the Segregation of duties principle.

d) Vulnerabilities of ICS assets should be considered security sensitive information and classified and controlled using company established policies, procedures, and protection methods, at rest in all forms including paper and in transit.

e) It should be noted that both architectural and software security flaws are potential sources of vulnerabilities (e.g. insufficient security zone network segmentation)

### 6.5.5 ID.RA-2 – Threat Intel Sharing Forums and Sources

Cybersecurity threat intelligence gathered from both internal and external sources can provide valuable insight on threats and vulnerabilities. On-going review and assessment of such intelligence can assist an organization with maintaining awareness of the threat landscape and the application of risk management processes. Cybersecurity threat intelligence should be actively pursued, cataloged, and assessed to maintain the desired risk posture.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); (6); (7); |

#### 6.5.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires the cataloging of all received threat intelligence, regardless of source.

2) The IAC Cybersecurity Plan requires that risk management processes identify risk to all cataloged threat intel associated with unauthorized disclosure and modification.

3) The IAC Cybersecurity Plan requires that the IAC Cyber threat intelligence catalog be classified according to identified risk.

4) The IAC Cybersecurity Plan requires that the threat intel catalog retains the information classification label as specified by the source of the threat intel.

5) The IAC Cybersecurity Plan requires that the IAC Cyber threat intel catalog be protected according to information classification and the requirements specified by the source of the threat intel.

#### 6.5.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.5.5.3 Extended Profile Requirements

6) The IAC Cybersecurity Plan requires that IAC cybersecurity risk management processes use external cyber threat intelligence information sharing forums and sources.

7) The IAC Cybersecurity Plan requires that IAC cybersecurity risk management processes include sharing of Threat intelligence received from external sources with organizationally defined personnel.

#### 6.5.5.4 Supplemental Guidance

a) Oil and Gas owner/operators, and IT and IAC technology supply chain vendors should strongly consider joining and actively participating in the Oil and Gas Information Sharing and Analysis Center (ONG-ISAC). Contact American Petroleum Institute or other oil and gas trade institute for more information.

### 6.5.6 ID.RA-3 – Internal and External Threat Identification

Applying consistent threat identification criteria is fundamental to effective tailored risk assessments. Inaccuracies can result in missed threats, poorly mitigated vulnerabilities, and an unbalanced security posture that may be inconsistent with an organization's risk tolerance. Threat and threat analysis should be cataloged and classified to ensure that analysis can be later referenced or modified as new threats develop or existing threats change.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (14); |

#### 6.5.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires the cataloging of identified threats to IAC Segregated Environments.
2) The IAC Cybersecurity Plan requires that consistent criteria be established to identify IAC threats.
3) The IAC Cybersecurity Plan requires that the identification of threats include IAC cybersecurity assessment activities (e.g. threat modeling, pen test, Red-team, Blue-team, internal audits, etc.).
4) The IAC Cybersecurity Plan requires that consistent criteria be established to assess and categorize (e.g. type, credibility rating, etc.) identified threats.
5) The IAC Cybersecurity Plan requires that the threats be categorized as current or emerging threats.
6) The IAC Cybersecurity Plan requires that the identification and categorization of threats includes the assessment of the attack vector origin identifier attributes of internal, external, and supply chain.
7) The IAC Cybersecurity Plan requires that the identification and categorization of threats includes the assessment of the identifier attributes for actions of people including inadvertent actions, inactions and deliberate actions taken from internal, external, and supply chain attack vectors.
8) The IAC Cybersecurity Plan requires that the identification (e.g. name, tag, label, etc.), assessment results, and categorization attributes of the threats are included in the IAC threats catalog.
9) The IAC Cybersecurity Plan requires that risk management processes identify risk to the threat catalog associated with unauthorized disclosure and modification.
10) The IAC Cybersecurity Plan requires that the threat catalog be classified according to identified risk.
11) The IAC Cybersecurity Plan requires that the IAC Cyber threat intel catalog be protected according to information classification.
12) The IAC Cybersecurity Plan requires that the threat catalog be refreshed periodically.

#### 6.5.6.2 Enhanced Profile Requirements

13) The IAC Cybersecurity Plan requires that that Cyber Threat Intelligence be assessed for relevance and applicability to Enhanced Profile IAC Cyber Environments.

#### 6.5.6.3 Extended Profile Requirements

14) The IAC Cybersecurity Plan requires that that Cyber Threat Intelligence be assessed for relevance and applicability to Extended Profile IAC Cyber Environments.

#### 6.5.6.4 Supplemental Guidance

a) A good reference for the consistent risk assessment categorization criteria is the Technical Report: A Taxonomy of Operational Cyber Security Risks Version 2, Software Engineering Institute CMU/SEI-2014-TN-006, copyright 2014 Carnegie Mellon University.

### 6.5.7 ID.RA-4 – Potential Impacts and Likelihoods

Knowledge of cybersecurity threats alone is insufficient for providing a comprehensive view of the risks to an organization’s IAC Cyber Environment. Consideration should be given to determining the impact of a successful compromise as well as the likelihood of a compromise occurring. Both are fundamental to an effective risk assessment process and including these factors can result in assessment outcomes, which are better aligned with an organization’s risk tolerance.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); |

#### 6.5.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC risk assessment process include the impact and likelihood of potential compromises to availability, integrity and data security from threats acting on vulnerabilities of IAC Segregated Environments.
2) The IAC Cybersecurity Plan requires that consistent criteria be established to identify potential impacts caused by compromises to IAC vulnerabilities

3) The IAC Cybersecurity Plan requires that impact assessment artifacts be risk-appropriately classified using a company defined information classification process.
4) The IAC Cybersecurity Plan requires that impact assessment artifacts be protected in accordance with its information classification.
5) The IAC Cybersecurity Plan requires that consistent criteria be established to estimate the likelihood of potential compromises from IAC vulnerabilities.
6) The IAC Cybersecurity Plan requires that likelihood estimate artifacts be classified using an information classification process.
7) The IAC Cybersecurity Plan requires that likelihood estimate artifacts be protected in accordance with its information classification.
8) The IAC Cybersecurity Plan requires the implementation of a formal impact assessment process.
9) The IAC Cybersecurity Plan requires that the impact assessment process include the identification and categorization of business objectives.
10) The IAC Cybersecurity Plan requires that the impact assessment process include the identification and categorization of potential impacts to business objectives.
11) The IAC Cybersecurity Plan requires that the impact assessment process include the identification and categorization of business objective impact severity levels.
12) The IAC Cybersecurity Plan requires that the impact assessment process include the mapping of business objective impact severity levels to security assurance levels for required minimum security requirements selection (i.e. API 1164 Profile Selection).
13) The IAC Cybersecurity Plan requires that IAC Stakeholders responsible for the IAC impact assessments are, at minimum, consulted and informed through formalized management-of-change processes on any modification that could affect the impact to business objectives or impact business objective impact severity level of the IAC Cyber Environment.

#### 6.5.7.2 Enhanced Profile Requirements

14) The IAC Cybersecurity Plan requires that business objective impact assessment recurs periodically.

#### 6.5.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.5.7.4 Supplemental Guidance

a) See section 4.4.2 Security Requirements to Business Objectives Mapping on page 12 above for guidance on business objective impact mapping to security control selection. Using business objectives from above, identify any additional business objectives.
b) Vetted and applicable threat intelligence should be considered security sensitive information and classified and controlled using company established policies, procedures, and protection methods, at rest in all forms including paper and in transit.

### 6.5.8 ID.RA-5 – Risk Determination

When determining risk, an organization should understand that risk impact draws upon knowledge of existing technical and business environments. Risk likelihood draws on the threat landscape and as well as existing vulnerabilities. The objective of risk determination is to assess likelihood and impact factors to ascertain the prescribed risk response (i.e. Treat, Tolerate, Transfer, or Terminate) that aligns with the organization's risk strategy.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 6.5.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the risk determination process incorporate a documented impact assessment.
2) The IAC Cybersecurity Plan requires that the risk determination process incorporate a documented likelihood assessment process.

3) The IAC Cybersecurity Plan requires that consistent criteria be established for determining the rating of risks.
4) The IAC Cybersecurity Plan requires that the risk determination process incorporate results of physical security assessments and Health Safety and Environment (HSE) assessments to determine the comprehensive risk.
5) The IAC Cybersecurity Plan requires that IAC Stakeholders responsible for the IAC risk assessments are, at minimum, consulted and informed through formalized management-of-change processes on any modification that could affect the risk to business objectives from the IAC Cyber Environment.

#### 6.5.8.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.5.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.5.9 ID.RA-6 – Responding to Risk

Completion of a risk assessment process should result in the selection of response elements. Once a risk is identified, organizations should evaluate the presence and severity of the risk and balance that against their tolerance for that risk. Comparison of the two should provide direction for action (if any) to minimize risk outside the organization’s tolerance level. Specific mitigations for that risk should be developed, prioritized, and implemented.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 6.5.9.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the risk assessment process determines risk response options.
2) The IAC Cybersecurity Plan requires that the risk assessment process prioritizes risk response options.
3) The IAC Cybersecurity Plan requires that management who is accountable for the safety, integrity and reliability of the IAC Segregated Environment shall review and approve the results of the risk assessment prior to any risk response action is taken that affects the IAC Security Zone.

See 6.5 IAC Risk Assessment (ID.RA) Baseline Profile Requirements on page 36 above.

#### 6.5.9.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.5.9.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.5.9.4 Supplemental Guidance

a) If the risk exposure is greater than the risk tolerance, then actions should be taken to address the risk. These actions could be to terminate the risk, transfer the risk, or treat the risk to reduce it to an acceptable level. If the risk exposure is below the risk appetite than the response can be to tolerate the risk.

## 6.6 Asset Management (ID.AM)

Asset management is a primary activity in any security program to ensure appropriate security controls are implemented across all cyber assets of the organization.

| | | |
|---|---|---|
| **P1** (1); | **P2** (1); | **P3** (1); |

### 6.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires the IAC Cybersecurity Plan include an IAC Cyber Asset Management program to manage physical IAC Cyber Assets, logical IAC Cyber Assets, IAC software and firmware assets, data flows, external system dependencies, and the associated cybersecurity roles and responsibilities.

### 6.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.6.4 ID.AM-6 – Cybersecurity Roles and Responsibilities

One of the first IAC Cyber Environment assets to be identified are individuals and their cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) to ensure responsivity of and accountability for cybersecurity tasks are unambiguously established and those that should be informed or consulted on cybersecurity activities are sufficiently engaged.

The objective of Cybersecurity Roles and Responsibilities is to identify the personnel who will be responsible for implementing, managing, and monitoring cybersecurity processes in the IAC Cyber Environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 6.6.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that cybersecurity roles and responsibilities for all IAC Cyber Environments are documented.
2) The IAC Cybersecurity Plan requires that the cybersecurity responsibilities be allocated to roles and assigned within the Company’s workforce and within third-party stakeholders.
3) The IAC Cybersecurity Plan requires that the role assignment includes the alignment of the responsibilities with the capability of assigned personnel.

#### 6.6.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.6.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.6.4.4 Supplemental Guidance

a) There should be special consideration of the alignment of IAC operational knowledge and responsibilities and the skills required for cybersecurity roles such that a cybersecurity role is co-assigned to both an Ops and a Security personnel who work in partnership on the tasks.
b) Managing relationships with third parties can be especially challenging. Having a consistent organizational point of contact for third party relationships can help with clear and consistent communications.

### 6.6.5 ID.AM-1 – IAC Cyber Asset Inventory

Without a comprehensive inventory of the physical IAC Cyber Assets that comprise the IAC Cyber Environment(s), it is difficult to assess where security measures are applied and to prioritized where they will have the greatest impact. The inventory should be the basis for decisions made regarding the relative risk imposed on the essential functions of the IAC Cyber Environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 6.6.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cyber Asset management plan exists to manage physical and virtual asset tracking and reporting of IAC Cyber Assets.
2) The IAC Cybersecurity Plan requires that consistent criteria be established for the identification of physical IAC Cyber Assets.
3) The IAC Cybersecurity Plan requires that virtual assets hosted by physical assets are considered separate assets for the purposes of the physical asset inventory.
4) The IAC Cybersecurity Plan requires that a minimum set of asset inventory attributes be established to support effective physical asset tracking and reporting including a unique identifier (e.g. organizational responsibilities, manufacturer, model, serial numbers, etc.)

5) The IAC Cybersecurity Plan requires that the physical inventory includes the IAC Security Zone or Conduit to which the IAC Cyber Asset belongs.

#### 6.6.5.2 Enhanced Profile Requirements

6) The IAC Cybersecurity Plan requires that the physical asset inventory identifies the asset owner.

#### 6.6.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.6.5.4 Supplemental Guidance

a) The suggested physical inventory attributes including the following: Unique identifier/asset tag, Asset Owner, Asset Administrator, Manufacturer, Model, Firmware version, IP Address, MAC Address, Site/Location, General Description, System, End of Support, End of Life,.

b) Inventory should not individual instruments that are not network connected.

c) Pipeline control systems and components include, but are not limited to, SCADA System servers, data concentrators, protocol converters, Control Room equipment, Consoles, Programable logic controllers (PLCs), Remote Terminal Units (RTUs), Flow Computers, Human Machine Interfaces (HMIs) Remote Operated Values, sensors, actuators, IIoT devices, network devices (routers, switches, hubs), terminal servers, 3rd party communication service provider equipment (VSAT Satellite, cellular modems, microware circuit demarcation equipment).

d) Organization should consider passive, automated mechanisms for maintaining the physical asset inventory. Commercial systems exist that can collect hardware inventory by monitoring network dataflows. This technology can be especially helpful in highly distributed applications, such as a pipeline, to collect inventory from multiple nonlocal stations and return the inventory to a central repository. They may also provide alerts for unplanned inventory change events or unknown devices connected to the network.

e) Organizations should consider including spares and replacements in the physical asset inventory.

#### 6.6.5.5 Hazardous Liquid Pipeline Supplemental Guidance

f) Hazardous Liquid Pipeline IAC Cyber Assets and IAC Cyber Systems also include, but are not limited to pump controllers, tank sensors, leak detection systems, and leak detection sensors.

#### 6.6.5.6 Natural Gas Pipeline Supplemental Guidance

g) Natural Gas Pipeline IAC Cyber Assets and IAC Cyber Systems also include, but are not limited to meter station automation, compressor station automation, and leak detection systems.

#### 6.6.5.7 IIoT Cautions and Supplemental Guidance

h) IIoT systems' high device counts, low cost, and potentially disposable hardware impose new challenges for inventory tracking and management. See NIST 8228 for additional details.

### 6.6.6 ID.AM-2 – Software Asset Catalog

Without a comprehensive catalog of the software, firmware, middleware, executables, and applications (herein collectively referred to as software) that comprise the control systems, it is difficult to assess where security measures are required, and address identified potential software vulnerabilities. The inventory will be the basis for decisions made regarding the relative risk introduced into the essential functions of the IAC Cyber Environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); |

#### 6.6.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cyber Asset management plan exists to manage cataloging, tracking, and reporting of software used in the IAC Cyber Environment.

2) The IAC Cybersecurity Plan requires that all software required for the operation of IAC essential functions are included in the IAC software asset catalog.

3) The IAC Cybersecurity Plan requires that a minimum set of software asset attributes to support effective asset tracking and reporting are included in the IAC software asset catalog (e.g. organizational responsibilities, manufacturer, version and revision numbers, license keys, etc.).

4) The IAC Cybersecurity Plan requires that the software asset attributes specify IAC essential function dependencies.

#### 6.6.6.2 Enhanced Profile Requirements

5) The IAC Cybersecurity Plan requires that software asset catalog include the asset owner.
6) The IAC Cybersecurity Plan requires that the software asset catalog includes, at a minimum, attributes of Operating System manufacturer, product name, and version, and essential function apps/executables manufacturer, product name, and version.
7) The IAC Cybersecurity Plan requires that the software asset catalog includes software libraries w/versions and security services w/version (e.g. OpenSSL 1.2)
8) The IAC Cybersecurity Plan requires that the software asset catalog be aggregated into a central repository.

#### 6.6.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.6.6.4 Supplemental Guidance

a) The suggested physical inventory attributes including the following: Software License Number, Software License Owner, Software Version, Revision, Embedded OS Information, Manufacturer, Version/Revision/Build number, License expiration, End of Support, End of Life.
b) Automated methods to collect software inventory can negatively affect IAC Assets and care should be taken in the method selection.
c) An appliance with firmware should be counted in the physical asset inventory.

#### 6.6.6.5 IIoT Cautions and Supplemental Guidance

d) IIoT system's lightweight software, lack of dominant platforms, and immature software lifecycle impose new challenges for inventory tracking and management. For further information, see NIST 8228.

### 6.6.7 ID.AM-4 – Cataloging External Cyber Assets

Without a comprehensive inventory of all external Cyber Assets with dependencies on or from the IAC Cyber Environment it is difficult to ensure appropriate security measures are implemented to control availability, integrity, and data protection of the cyber asset. The catalog will be the basis for decisions made regarding the relative risk introduced into the essential functions of the component, device, or system.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 6.6.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cyber Asset management program exists to manage cataloging, tracking, and reporting of external systems that depend on the IAC Cyber Environment or on which the IAC environment depends as assets.
2) The IAC Cybersecurity Plan requires that consistent criteria be established to define the boundaries around the cyber asset’s security zone used in determining what is classified as an external Cyber Asset.
3) The IAC Cybersecurity Plan requires that external Cyber Asset systems that communicate with the IAC Cyber Environment are cataloged.
4) The IAC Cybersecurity Plan requires that external Cyber Assets that depend on the IAC Cyber Environment or on which the IAC Cyber Environment depends are cataloged, including the dependency.
5) The IAC Cybersecurity Plan requires that the external Cyber Asset catalog contains attributes that are sufficient in type and detail to support effective tracking and reporting.
6) The IAC Cybersecurity Plan requires that the external Cyber Asset catalog includes the purpose, the external Cyber Asset identification, the organizational owner, and the location information of the external Cyber Asset.

#### 6.6.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 6.6.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 6.6.7.4 Supplemental Guidance

a) To clearly identify what is considered an external system, consistent criteria must be established to define the security perimeter around the cyber asset. Establishing security zones by grouping IAC and related cyber assets using risk-based criteria, including, but not limited to, shared risk profile, physical or logical location, criticality of assets, operational function, physical and logical access requirements or responsible organization allows for risk-appropriate security measures to be applied both within the security zone and to the conduits used to communicate between security zones.

b) External flows mapped in ID.AM-3 may provide insight on where information is stored externally to the IAC Cyber Environment.

c) Information considered to be sensitive or security related base on criteria defined by the organization should be controlled. The security controls of the external information system should be evaluated to ensure the information is properly protected.

See PR.DS and PR.IP sections below

d) Some elements that may need be included in the catalog include but are not limited to, contact information, type of data stored, approved communication methods, contractual references.

### 6.6.7.5 IIoT Cautions and Supplemental Guidance

e) IIoT systems for pipelines will have additional challenges for third party and service providers that process IIoT-derived data. Companies should approve where their operational data is stored and processed.

### 6.6.8 ID.AM-3 –Communications and Data Flows

Without a comprehensive catalog of all communications and data flows with systems both outside and inside the IAC Security Zone, it is difficult to assess where security measures are required, and address identified potential vulnerabilities. The inventory should be the basis for decisions made regarding the relative risk introduced into the essential functions of the component, device, or system.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); |

### 6.6.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the communications and data flows that occur within an IAC Security Zone is cataloged.

2) The IAC Cybersecurity Plan requires that the communications and data flows that traverse an IAC Internal Conduit is cataloged.

3) The IAC Cybersecurity Plan requires that the communications and data flows that traverse an IAC Intermediate Conduit is cataloged.

4) The IAC Cybersecurity Plan requires that the communications and data flows that traverse an IAC External Conduit is cataloged.

5) The IAC Cybersecurity Plan requires that the communication and data flows catalog contain attributes that are sufficient in type and detail to support effective tracking and reporting.

6) The IAC Cybersecurity Plan requires that communications and data flows catalog identify any dependencies from IAC essential functions.

7) The IAC Cybersecurity Plan requires that communications and data flows that traverse an IAC External Conduit catalog the purpose, the external Cyber Asset identification, the organizational owner and location information of the external Cyber Asset.

8) The IAC Cybersecurity Plan requires that the communications and data flows catalog contain the approver of the communication and data flows.

#### 6.6.8.2 Enhanced Profile Requirements

9) The IAC Cybersecurity Plan requires that the communications and data flows catalog contain the security approver and the operations approver.
10) The IAC Cybersecurity Plan requires that communications and data flows that traverse an IAC External Conduit catalog the functions, ports, protocols, and services purpose required by IAC essential functions.

#### 6.6.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.6.8.4 Supplemental Guidance

a) Identification of data flow criticality may be helpful in prioritizing restoration and response efforts.
b) Both graphical and tabular methods should be considered when specifying the method used to map data flows.
c) IAC External Conduits are important because they can provide potential opportunity as an external attack vector. As such, the initial assessment and the review frequency for communications that traverse an IAC External Conduit should be prioritized.

#### 6.6.8.5 IIoT Cautions and Supplemental Guidance

d) Identify whether data flows cross international or regulatory boundaries (e.g., cloud data and processing may cause previously unidentified legal issues).

### 6.6.9 ID.AM-5 – Resource Prioritization

Security priorities describe the potential adverse impacts to operations, assets, and individuals if control systems are comprised through a loss of essential functions. Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, essential function performed, and business value. The categorization of cyber assets is crucial to applying cybersecurity measures.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 6.6.9.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires the implementation of a risk-based IAC Cyber Asset management plan to manage the prioritization of resources.
2) The IAC Cybersecurity Plan requires that consistent criteria be established for prioritizing IAC Cyber Assets based on their classification, criticality, and business value.
3) The IAC Cybersecurity Plan requires that resource prioritization criteria include dependencies and constraints associated with IAC Cyber Asset essential functions.
4) The IAC Cybersecurity Plan requires that that IAC Cyber Assets be prioritized according to the documented criteria.

#### 6.6.9.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 6.6.9.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 6.6.9.4 Supplemental Guidance

a) When restoration or mitigation efforts are needed, a prioritization method that guides where resources are applied first is essential. The mission of the organization should be the guiding principle for the prioritization.

## 7 ONG IAC Cybersecurity Profile Requirements - Protect (PR)

The purpose of the Protect Function is to develop and implement appropriate safeguards to control system essential functions to ensure delivery of critical services. The Protect Function supports the ability to reduce the impact of a potential cybersecurity event. The target profile outcome Categories and Subcategories within this Function are detailed below.

## 7.1 Access Control (PR.AC)

Access control is the protection of an IAC Cyber Asset's resources against unauthorized interaction. The objectives of access control are to block unauthorized access and to limit access from authenticated users, devices, and processes to only the resources required to perform their authorized functions or duties.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

### 7.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires the protection of IAC cyber assets against unauthorized physical and logical access to authorized actives and transactions consistent with the IAC Risk Management Strategy.
2) The IAC Cybersecurity Policy requires that no human user account credentials (e.g. user id and password) used for accessing an External Zone, or cyber assets therein, are also used as user account credentials for access to an IAC Segregated Environment.

### 7.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 7.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.1.4 PR.AC-5 – Network Integrity

Protecting network integrity is a foundational element of defending interconnected systems, especially within IAC Cyber Environments. A fundamental way to achieve this is through a defense-in-depth strategy that implements:

(1) Network Segmentation: IAC network(s) are divided into separately managed segments.

(2) Network Segregation: Different protection rulesets are defined using risk-based criteria and implemented to manage the security of each network segment.

It is this combination of network segmentation and segregation that defines security zones and the security conduits connecting them.

The objective of network integrity is to provide a segregated defense-in-depth approach to limit the attack surface of network interconnected IAC Cyber Assets from widespread horizontal and vertical movement of a potential network intrusion.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); (5); |

#### 7.1.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that any IAC Cyber Environment which is directly used in or in support of IAC essential functions be segregated into IAC Security Zones and IAC Security Conduits.
2) The IAC Cybersecurity Plan requires that all Cyber Assets deployed in any IAC Cyber Environment used directly in or in support of IAC essential functions are contained within (i.e. member of) an IAC Security Zone or IAC Security Conduit.
3) The IAC Cybersecurity Plan requires that authorization privileges for IAC Segregated Environment access accounts are managed for all interfaces that provide human user access.
4) The IAC Cybersecurity Plan requires that network architectural diagrams, including IAC Security Zone and IAC Security Conduit segmentations, are maintained.

#### 7.1.4.2 Enhanced Profile Requirements

5) The IAC Cybersecurity Plan requires that any external transport service provider used is included in applicable IAC Cyber Environment drawings.

#### 7.1.4.3 Extended Profile Requirements

6) The IAC Cybersecurity Plan requires that the IAC Security Zone and IAC Security Conduit drawings include each IAC Cyber Asset within the zone or conduit security perimeter.

#### 7.1.4.4 Supplemental Guidance

a) IAC Security Conduits should be designed to filter / block nonessential communication from reaching the IAC Cyber Assets that perform essential functions.

b) The organization should consider have the capability to identify and report unauthorized wireless devices transmitting within the IAC Segregated Environment perimeter, especially for those with an API 1164 Impact Rating of I2-Medium or higher.

#### 7.1.4.5 IIoT Cautions and Supplemental Guidance

c) Although IIoT devices may share IAC sensor inputs, they should not communicate with the core IAC Cyber Environment. IIoT devices should be in separate security zones from core IAC Cyber Environment if communications are absolutely required. The best practice in this case is to implement an Inter-IAC Cyber Environment security zone between the IAC security zone and the IIoT security zone.

### 7.1.5 PR.AC-1 – Access Control and Identity Lifecycle Management

Identity lifecycle management is a set of processes that manage digital identities from creation to deletion. The objective of digital identity lifecycle management is to ensure that digital access identities and credentials for authorized devices, users and processes are issued, managed, verified, revoked, and audited.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); |

#### 7.1.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that Identity Lifecycle Management processes exists which manage all human, device, and process accounts and associated credentials.

2) The IAC Cybersecurity Plan requires that all human users are identified and authenticated prior to logical access to an IAC Segregated Environment or IAC Cyber Asset within it on all interfaces that provide human user access (e.g. all interactive protocols on network interface, integrated console, serial console, programmer interface, etc.).

3) The IAC Cybersecurity Plan requires that human user shared (a.k.a. functional) accounts are managed consistent with the IAC Risk Management Strategy.

4) The IAC Cybersecurity Plan requires that user accounts that are no longer needed, for any reason, are rendered unusable for gaining access to an IAC Segregated Environment or IAC Cyber Asset within a time frame consistent with the IAC Risk Management Strategy.

5) The IAC Cybersecurity Plan requires that authenticators be protected from unauthorized disclosure and modification when at-rest and in-transit.

6) The IAC Cybersecurity Plan requires risk-appropriate authenticator strength (complexity, length, reuse, digital key expiration, etc.) consistent with the IAC Risk Management Strategy.

7) The IAC Cybersecurity Plan requires the modification of default user accounts shipped with devices or created during device resets prior to use in an IAC Security Zone.

#### 7.1.5.2 Enhanced Profile Requirements

8) The IAC Cybersecurity Plan requires that, where technically supported, all human users are uniquely identified and authenticated prior to accessing an IAC Cyber Asset or IAC Security Zone.

9) The IAC Cybersecurity Plan requires that where unique human user identification and authentication is not technically supported, risk appropriate compensating controls are implemented consistent with the IAC Risk Management Strategy.

10) The IAC Cybersecurity Plan requires that identity and credential management processes generate log events (e.g. failed authentication attempts).

11) The IAC Cybersecurity Plan requires that identity and credential log events contain sufficient detail to support auditing requirements consistent with the IAC Risk Management Strategy.

#### 7.1.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.1.5.4 Supplemental Guidance

a) Within an IAC Cyber Solution, processing tasks used for IAC essential functions may be required to execute using highly privileged access. These cases may have the inadvertent unintended consequences of violating the least-privilege principle. Organizations should strongly consider additional compensating controls for these situations.

b) Special consideration should be given to service account as they present multiple challenges. Managing service passwords may cause downtime. Disabling or otherwise prohibiting interactive login for service accounts should strongly be considered.

c) Lifecycle management requirements of shared accounts (i.e. functional accounts) can present multiple security challenges. A list of users with access to shared (aka functional) accounts should be managed.

### 7.1.6 PR.AC-6 – Access Non-repudiation

Non-repudiation refers to the principle that a user is who the user claims to be, and that the user's identify and credentials are only known to this user, therefore, any interactions conducted using those credentials are ensured to be interactions made by that user. This is achieved by proofing the identity, binding the real-life identity to a digital identity (user credential confidentiality), and asserting that digital identity in the form of access control authentication for all interactions with the cyber asset, IAC Cyber Asset, or IAC System.

Identity proofing is a process that verifies and authenticates the identity of an individual thereby matching a person's real identity to their claimed identity. That is, it verifies that they are actually who they say they are. The identity proofing process has three distinct parts:

(1) Identity Resolution: Core attributes and evidence is collected. This uniquely distinguishes a person's identity in the context of the relevant population.

(2) Identity Validation: Evidence is validated. Collected evidence from the real-life subject is checked for authenticity, validity, and accuracy.

(3) Identity Verification: Evidence is verified. Linkage between claimed and real identity is established and confirmed.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.1.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that risk-appropriate access non-repudiation protections are employed

2) The IAC Cybersecurity Plan requires that risk-appropriate identity proofing is employed.

3) The IAC Cybersecurity Plan requires the binding (confidentiality of credentials) of assigned unique digital identities (e.g. non-shared user accounts, security tokens, session keys) with real-life identities.

#### 7.1.6.2 Enhanced Profile Requirements

4) The IAC Cybersecurity Plan requires the employment of automated mechanisms to support assertion of identities in cyber asset, IAC Cyber Asset and IAC System interactions. (e.g. Security Assertion Markup Language [SAML], Kerberos tickets, security tokens, session keys, etc.).

#### 7.1.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.1.6.4 Supplemental Guidance

a) The IAC Cybersecurity Program should implement identity lifecycle management processes that ensure identity proofing practices comply with applicable privacy and civil rights laws and regulations.

### 7.1.7 PR.AC-7 – Risk Appropriate Authentication

The strength of user, device, and process authentication is a fundamental security attribute that is shared within a security zone. The strength of access controls to an IAC Segregated Environment should be directly proportional to the risk of unauthorized access to IAC essential functions directly in control of or supported by the IAC Cyber Assets within the IAC Segregated Environment. The objective of Risk Appropriate Authentication is to apply a consistent strength of authentication throughout an IAC Segregated environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.1.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that user, device, or process access to an IAC Segregated Environment employs an authentication strength that is risk-appropriate for the authorized interactions with the IAC Cyber Assets within the IAC Segregated Environment.
2) The IAC Cybersecurity Plan requires that user, device or process access to an IAC Cyber Asset employs an authentication strength that is risk-appropriate for the IAC essential functions directly in control of or supported by the IAC Cyber Assets within the IAC Segregated Environment.
3) The IAC Cybersecurity Plan requires that user, device, or process access requires consistent authentication strength to IAC Cyber Assets within the same IAC Segregated Environment.
4) The IAC Cybersecurity Plan requires that compensating controls be employed when user, device or process authentication strength cannot be implemented consistently within a Segregated Environment.

#### 7.1.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.1.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.1.7.4 Supplemental Guidance

a) The organization should strongly consider the use of two-factor authentication for nonlocal access to all IAC Cyber Environments which have IAC essential functions.
b) Shared or functional user accounts are often used in IAC Cyber Environments for a variety of reasons. These types of accounts violate the security principle of nonrepudiation and can violate the principle of least-functionality. These types of user accounts can make it exceedingly difficult to track what activity is authorized versus unauthorized. Organizations should strongly consider implementing alternate authentication and authorization methods other than shared or functional user accounts. Where alternate methods cannot be implemented, organizations should strongly consider additional compensating controls be implemented.

### 7.1.8 PR.AC-4 –Access Authorization

In an IAC Cyber Environment, it is critical to essential function security to ensure the right people have access to the correct information, functions and systems and are not blocked from their tasks due to lack of authorization. It is also essential that individuals are not authorized to access resources, especially IAC essential functions, that are not required for their approved job functions.

It is also critical that the authorization strategy implements a separation of duties model (e.g. administration, security administration, operations, etc.) to ensure safety, security, and operational safeguards cannot be bypassed. The objective of access authorization is to ensure permissions are managed, incorporating the principles of least privilege and segregation of duties.

NOTE Safety implications are an important consideration when developing the authorization strategy.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 7.1.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that authorization privileges for IAC Cyber Asset access accounts are managed for all interfaces that provide human user access.
2) The IAC Cybersecurity Plan requires that access privileges to IAC Cyber Assets are manage based on user roles (e.g. system admins, security admins, technicians, nonlocal access user, etc.).
3) The IAC Cybersecurity Plan requires that the least privilege principle be used for authorization provisioning for IAC Cyber Asset access user roles.

4) The IAC Cybersecurity Plan requires that the segregation of duties between user roles are defined for IAC Cyber Asset access user roles.
5) The IAC Cybersecurity Plan requires that the assigned privileges do not violate segregation of duties for authorization provisioning of IAC Cyber Asset access user roles.
6) The IAC Cybersecurity Plan requires that compensating controls be employed in cases where segregation of duties is not implementable (e.g. insufficient personnel for unique role assignments).

#### 7.1.8.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.1.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.1.9 PR.AC-3 – Nonlocal Access Management

Nonlocal access is any human user access to an IAC Cyber Asset using network communications whether originating from inside an IAC Security Zone or an External Zone. Nonlocal access does not include individuals physically present and physically connected to an IAC Cyber Asset.

Proper authentication and logging of nonlocal access to IAC Cyber Assets should be deployed to detect user intrusion. Nonlocal access to IAC Cyber Assets is a potential attack vector for which malicious activity can be nonlocally activated to launch an attack on the IAC System.

The objective of Nonlocal Access Management is to mitigate the risk of unauthorized access through management of nonlocal connections using active approval chain(s), strong authenticators, session management, and log auditing.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); |

#### 7.1.9.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that consistent criteria be used to define the security boundaries around the IAC Segregated Environments to identify the scope of nonlocal access controls.
2) The IAC Cybersecurity Plan requires that all methods of nonlocal access to IAC Segregated Environments are managed.
3) The IAC Cybersecurity Plan requires that nonlocal access approvals be managed.
4) The IAC Cybersecurity Plan requires that consecutive authentication failures using a nonlocal access account is managed in alignment with the IAC Risk Management Strategy.
5) The IAC Cybersecurity Plan requires processes to manually manage nonlocal access sessions (e.g. enable, terminate, reauthentication, etc.).
6) The IAC Cybersecurity Plan requires processes to automatically manage nonlocal access sessions (e.g. enable, session duration, session inactivity timeout termination, reauthentication etc.).
7) The IAC Cybersecurity Plan requires that nonlocal access during emergency response situations are defined (e.g. system outages, cyber incident responses, physical incident responses, etc.)
8) The IAC Cybersecurity Plan requires that an access log retention schedule be defined for IAC nonlocal access.

#### 7.1.9.2 Enhanced Profile Requirements

9) The IAC Cybersecurity Plan requires that nonlocal access communications be encrypted when traversing an IAC External Conduit.
10) The IAC Cybersecurity Plan requires that nonlocal access by third parties (e.g. vendors, service providers, etc.) is approved by the IAC security function and the IAC operations function.
11) The IAC Cybersecurity Plan requires that the allowed actions, functions, or transactions executed by nonlocal access sessions are defined (e.g. read only monitoring, configuration changes, nonlocal programming, manipulation of control system functions, etc.).

#### 7.1.9.3 Extended Profile Requirements

12) The IAC Cybersecurity Plan requires that technical controls be implemented to prevent unauthorized actions, functions, and transaction from nonlocal access sessions.

### 7.1.10 PR.AC-2 – Physical Access Management

Physical security management employs measures that help ensure that all IAC Cyber Assets are protected physically from unauthorized access, damage, misuse, and loss. The objective of Physical Access Management is to create and manage a secure environment in which the IAC Cyber Assets operate by limiting physical access to those authorized.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); |

#### 7.1.10.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a formal physical security plan exists which defines risk-based processes and operational and procedural controls to manage physical access at sites with one or more IAC Cyber Assets.
2) The IAC Cybersecurity Plan requires that the physical access management plan aligns to the level of risk identified with the highest-level IAC Segregated Environment Profile located at the site.

#### 7.1.10.2 Enhanced Profile Requirements

3) The IAC Cybersecurity Plan requires that the physical access management plan implement a least privilege model (i.e. limits access to only areas required to perform authorized duties.)
4) The IAC Cybersecurity Plan requires that the physical access management plan specifies operational and procedural controls to manage logs for physical access to IAC Cyber Assets (e.g. sign-in paper logs; digitally recorded electronic badge in/out events).
5) The IAC Cybersecurity Plan requires that the physical access management plan specifies access processes during emergency response situations (e.g. access by first responders, site containment, etc.)
6) The IAC Cybersecurity Plan requires that the physical access management plan specifies layered physical barrier requirements for access to IAC Cyber Assets that support or perform essential functions commensurate to the risk of unauthorized access to those assets (e.g. SCADA control center, DCS control room, Meter/ROV station)
7) The IAC Cybersecurity Plan requires that the physical security plan specifies electronic monitoring and alerting processes.

#### 7.1.10.3 Enhanced Profile Requirements

8) The IAC Cybersecurity Plan requires that the physical access management plan specifies electronic monitoring and alerting processes.

#### 7.1.10.4 Supplemental Guidance

a) All physical security plans should be developed by the company's physical security function. Inclusion of the cybersecurity requirements within the physical security plan should be a collaborative effort between the physical security, cybersecurity, and IAC operation functions.
b) Requiring personnel to pass a back-ground check prior to physical access to a site that contains one or more IAC Cyber Assets that are part of an Enhanced Profile or Extended Profile IAC Segregated Environment may be considered to be an optional access control requirement.
c) Within a pipeline IAC Cyber Environment, there often exists IAC Segregated Environments (or portions thereof) that typically do not have personnel on-site. In such cases, prevention of unauthorized physical access may not be possible. For these pipeline sites, organizations should consider additional monitoring and detection mitigating controls.

## 7.2 IAC Cybersecurity Awareness and Training (PR.AT)

People, processes, and technology are the three pillars of a successful defense-in-depth security strategy. A successful IAC security program should not only focus on processes and technology controls. It should heavily focus on the human element, which is the most often targeted attack vector because it is often the easiest and most successful. An ecosystem of well informed and formally trained stakeholders can be one of the best defenses against both external, and intentional and unintentional internal cyber threats. The IAC stakeholder community consists of authorized users to access the IAC Cyber Environment (employees and contractors), company management with direct line responsibilities for the IAC Cyber Environments, senior executives with decision making responsibility that can influence the security posture of the IAC Cyber Environments, and 3rd party partners and vendors.

The objective of IAC Cybersecurity Awareness and Training is to provide cybersecurity awareness education and formal training to the organization's IAC stakeholder.

### 7.2.1 PR.AT-1 – IAC User Cyber Training

Users with authorization for direct interaction with any IAC Segregated Environment or its components are informed and trained.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.2.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a formal IAC cyber security training program exists for all IAC users and stakeholders.
2) The IAC Cybersecurity Plan requires that role-appropriate training be satisfactorily completed periodically at a risk-appropriate frequency based on IAC user role.
3) The IAC Cybersecurity Plan requires that risk and role-appropriate training be satisfactorily completed prior to accessing any IAC security zone or its components.
4) The IAC Cybersecurity Plan requires that training includes risk-appropriate behaviors and responses for all IAC users during both physical and cyber emergency situations.

#### 7.2.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.2.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.2.1.4 Supplemental Guidance

a) Consideration should be given to specific cyber training requirements for the different IAC Security Zone types deployed within the IAC Cyber Environment.
b) Organizations should consider cybersecurity awareness training that includes users recognizing and reporting potential indicators of insider threat.

#### 7.2.1.5 IIoT Cautions and Supplemental Guidance

c) It is strongly recommended that personnel responsible for implementation or maintenance of IIoT devices be required to take general IAC cyber-training and cyber-training focused on the potential risks to IAC Cyber Environments from internet enabled technology.

### 7.2.2 PR.AT-2 – IAC High Privileged Account User Cyber Training

The objective of IAC High Privileged Account User Cyber Training is to ensure that users with high privileged account access authorization for direct administrative interaction with any IAC Security zone or its components are trained for their roles and responsibilities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.2.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a formal IAC cyber security training program exists for all high privileged account users.
2) The IAC Cybersecurity Plan requires that role-appropriate training for high privileged account users is satisfactorily completed periodically at a risk-appropriate frequency based on IAC user role.
3) The IAC Cybersecurity Plan requires that risk and role-appropriate training be satisfactorily completed prior to administering any IAC Segregated Environment.

4) The IAC Cybersecurity Plan requires that training includes risk-appropriate behaviors and responses for IAC high privileged account users during both physical and cyber emergency situations.

#### 7.2.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.2.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.2.2.4 Supplemental Guidance

a) The types of Security zones defined within the IAC Cyber Environment may provide insight into role specific cyber training requirements.

b) Cybersecurity awareness training includes recognizing and reporting potential indicators of insider threat.

#### 7.2.2.5 IIoT Cautions and Supplemental Guidance

c) It is strongly recommended that personnel responsible for implementation or maintenance of IIoT devices be required to take general IAC cyber-training and cyber-training focused on the risk to IAC Cyber Environments from internet enabled technology.

### 7.2.3 PR.AT-3 – IAC Third-party Stakeholder Cyber Training

The objective of IAC Third-party Stakeholder Cyber Training is to ensure users with access to direct administrative interaction with any IAC Segregated Environment are trained for their roles and responsibilities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 7.2.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a formal IAC cyber security training program exists for all IAC third-party stakeholders.

2) The IAC Cybersecurity Plan requires that IAC cybersecurity awareness training for all IAC third-party stakeholders are contractually bound.

3) The IAC Cybersecurity Plan requires that third-party stakeholders' acknowledgement and agreement to abide by the organizations IAC security policies and procedures.

4) The IAC Cybersecurity Plan requires that role-appropriate training for IAC third-party stakeholders is satisfactorily completed prior to access any IAC Segregated Environment.

5) The IAC Cybersecurity Plan requires that IAC third-party stakeholder training includes risk-appropriate behaviors and responses during both physical and cyber emergency situations.

#### 7.2.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.2.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.2.3.4 Supplemental Guidance

a) The types of Security zones defined within the IAC Cyber Environment may provide insight into role specific cyber training requirements.

b) Cybersecurity awareness training includes recognizing and reporting potential indicators of insider threat.

#### 7.2.3.5 Natural Gas Transmission Pipeline Supplemental Guidance

c) Special consideration should be given to IAC third-party stakeholder cyber training regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 7.2.4 PR.AT-4 – IAC Management and Executive IAC Stakeholder Training

It is critical that company management, with direct line responsibilities for the IAC Cyber Environments and senior executives, are trained for their cybersecurity roles and responsibilities. This is to help ensure that they understand the nature and extent of any IAC cybersecurity risk decision they are required to make.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.2.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a formal IAC cyber security training program exists for all direct line IAC managers and senior executives.
2) The IAC Cybersecurity Plan requires that role-appropriate training be satisfactorily completed periodically at a risk-appropriate frequency based on management and executive roles.
3) The IAC Cybersecurity Plan requires that training includes roles and responsibilities for all direct line IAC managers and senior executives including during both physical and cyber emergency situations.
4) The IAC cybersecurity training program specifies the processes to ensure training includes regulatory requirements and risks for all direct line IAC managers and senior executives.

#### 7.2.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.2.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.2.5 PR.AT-5 –Physical Security and Cybersecurity Personnel Training

Physical and cybersecurity personnel with responsibilities for IAC Cyber Environments are trained for their roles and responsibilities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 7.2.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that roles and responsibilities training occur for all physical security and cybersecurity personnel with responsibilities for IAC Cyber Environments.
2) The IAC Cybersecurity Plan requires that risk and role-appropriate training be satisfactorily completed prior to administering any IAC security zone or its components for IAC cybersecurity personnel.
3) The IAC Cybersecurity Plan requires that role-appropriate training for physical and cybersecurity personnel is satisfactorily completed periodically at a risk-appropriate frequency based on IAC role.
4) The IAC Cybersecurity Plan requires that training includes roles and responsibilities, including during both physical and cyber emergency situations, for physical and cybersecurity personnel with responsibilities for IAC Cyber Environments.
5) The IAC Cybersecurity Plan requires that training includes risk-appropriate behaviors and responses during both physical and cyber emergency situations for physical and cybersecurity personnel with responsibilities for IAC Cyber Environments.

#### 7.2.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.2.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.2.5.4 Supplemental Guidance

a) The types of Security zones defined within the IAC Cyber Environment may provide insight into role specific cyber training requirements.
b) Cybersecurity awareness training includes recognizing and reporting potential indicators of insider threat.

c) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to receive or develop cybersecurity training relevant to the IAC Cyber Solution elements provided.

## 7.3 Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. The objective of Data Security is to ensure that data stored in or transferred into, out of, or within the IAC Cyber Environment that needs protection is documented and adequately protected.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); |

### 7.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires the protection from unauthorized access and modification of IAC information and records consistent with the IAC Risk Management Strategy.

2) The IAC Cybersecurity Plan requires that IAC data be classified by its protection requirements.

3) The IAC Cybersecurity Plan requires that all IAC information classifications include the data states of data-at-rest, data-in-transit, or data-in-use.

4) The IAC Cybersecurity Plan requires that the IAC information classification includes any IAC essential function dependencies.

5) The IAC Cybersecurity Plan requires the establishment of data protection requirements for all IAC information classifications.

6) The IAC Cybersecurity Plan requires the protection of all IAC information classifications according to their data protection requirements.

### 7.3.2 Enhanced Profile Requirements

7) The IAC Cybersecurity Plan requires that IAC executable files be included as a data type requiring protection.

### 7.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.3.4 Supplemental Guidance

a) Both the asset owner and the service provider should collaborate to identify control system data that needs protection.

b) The following data types should be included in the information classification protection process: executables, configuration data, user credentials, audit and security logs, test data, cryptographic keys, personally Identifiable Information (PII), proprietary data, including production data and trade secret data.

### 7.3.5 PR.DS-1 – IAC Data-at-Rest Protection (Inactive-Data)

IAC Data-at-rest is data that is not currently being transmitted across a network or actively being read or processed by an IAC Cyber Asset. Data-at-rest refers to inactive IAC data stored in any form that is used directly or indirectly by IAC Cyber assets in performance of IAC automated processes. Also included is data about the IAC system, stored in any form. (e.g. network architecture diagrams). It can be data stored on hard drives, solid state drives, backup archive media, and memory (e.g. RAM Drive). The data can be either onsite or offsite from where it can be put into an active state. It can be in fixed devices, portable devices, mobile devices, and removable devices. The objective of IAC Data-at-Rest Protection is to prevent unauthorized access and modification using risk-appropriate measures.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (5); |

#### 7.3.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that all IAC data-at-rest be authorized, validated, and protected for confidentiality, integrity, and availability from unauthorized access according to its information classification protection requirements.

2) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest originating from or stored in a Baseline Profile IAC Security Zone.

#### 7.3.5.2 Enhanced Profile Requirements

3) The IAC Cybersecurity Plan requires that IAC executables files be classified and protected by data-at-rest protection requirements.
4) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest originating from or stored in an Enhanced Profile IAC Security Zone.

#### 7.3.5.3 Extended Profile Requirements

5) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest originating from or stored in an Extended Profile IAC Security Zone.

#### 7.3.5.4 Supplemental Guidance

a) Data classifications and the associated data-at-rest protections should also include the classification and protection of both digital and printed IAC technical descriptions, including but not limited to design and as-built documentation of IAC Cyber Environments, network topology diagrams or schematics, IP addressing schemas, Wireless Site Surveys and configuration, network assessments, security assessment or penetration testing, and any other IAC engineering/implementation data controlled by a “need-to-know” principle.

#### 7.3.5.5 Natural Gas Transmission Pipeline Supplemental Guidance

b) Special consideration should be given to data-at-rest protection regarding FERC’s Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 7.3.6 PR.DS-2 – IAC Data-in-Transit Protection (Active-Data)

Data in transit is data that is currently traveling across a network between the data’s source and destination. This data can be moving across cables and wireless transmission. The objective of Data-in-Transit Protection is to prevent unauthorized access and modification of data traversing a network using risk-appropriate measures.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (5); (6); (7); (8); (9); (10); (11); (12); (13); | **P3:** (1); (2); (5); (6); (7); (8); (9); (11); (12); (14); (15); (16); (17); (18); (19); (20); |

#### 7.3.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that all IAC data-in-transit be authorized, validated, and protected for confidentiality, integrity, and availability from unauthorized access according to its information classification protection requirements.
2) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-in-transit originating from, destined for, and traversing through a Baseline Profile IAC Security Zone.
3) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for communications within a Baseline Profile IAC Security Zone
4) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an Internal Conduit between a Baseline Profile IAC Internal Zone and another Baseline Profile IAC Internal Zone.
5) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an Intermediate Conduit between a Baseline Profile IAC Internal Zone and an IAC Intermediate Zone.
6) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an IAC External Conduit between a Baseline Profile IAC Intermediate Zone and an IAC External zone.

#### 7.3.6.2 Enhanced Profile Requirements

7) The IAC Cybersecurity Plan requires that user sessions shall be classified and protected by data-in-transit protection requirements.

8) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-in-transit originating from, destined for, and traversing through an Enhanced Profile IAC Security Zone.

9) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for communications within an Enhanced Profile IAC security zone.

10) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an Internal Conduit between a Enhanced Profile IAC Internal Zone and another Enhanced Profile IAC Internal Zone.

11) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an IAC Intermediate Conduit between an Enhanced Profile IAC Security Zone and an Intermediate Zone.

12) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an IAC External Conduit between an Enhanced Profile IAC Intermediate Zone and an External Zone.

13) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an IAC Internal Conduit between an Enhanced Profile IAC Security Zone and a Baseline Profile IAC Security Zone.

#### 7.3.6.3 Extended Profile Requirements

14) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-in-transit originating from, destined for, and traversing through an Extended Profile IAC Security Zone.

15) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for communications within an Extended Profile IAC security zone.

16) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an Internal Conduit between an Extended Profile IAC Internal Zone and another Extended Profile IAC Internal Zone.

17) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an Intermediate Conduit between an Extended Profile IAC Security Zone and an IAC Intermediate Zone.

18) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing an IAC External Conduit between an Extended Profile IAC Security Zone and an External Zone.

19) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing a security conduit between an Extended Profile IAC Security Zone and a Baseline Profile IAC Security Zone.

20) The IAC Cybersecurity Plan requires that data-in-transit security requirements include the protections for IAC egress and IAC ingress communications traversing a security conduit between an Extended Profile IAC Security Zone and an Enhanced Profile IAC Security Zone.

#### 7.3.6.4 Natural Gas Distribution Pipeline Supplemental Guidance

a) Special consideration should be given to data-in-transit requirements, especially data flows to External Zones, regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information

### 7.3.7 PR.DS-3 – IAC Cyber Asset in Transition Protection

IAC Cyber Assets that are no longer needed, for any reason, resulting in removal, transfers, and disposition from the IAC Cyber Environment may contain sensitive information regardless of whether it was ever put into service in a production environment. The objective of IAC Cyber Asset in Transition Protection is to prevent sensitive data in an IAC Cyber Asset, which was used in or intended to be used in an IAC Cyber Environment, from being disclosed after the IAC Cyber Asset is no longer needed.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.3.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Asset management program addresses the asset lifecycle management requirements for disposal of IAC Cyber Assets that are no longer needed.
2) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest all for IAC Cyber Assets that are no longer needed.
3) The IAC Cybersecurity Plan requires that data protection requirements for the permanent removal of information from IAC Cyber Assets that are no longer needed is commensurate with the risk regardless of previous production use.
4) The IAC Cybersecurity Plan requires that Management of Change processes address, implement or otherwise align with IAC Cyber data protection requirements for IAC Cyber assets no longer needed.

#### 7.3.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.3.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.3.7.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to receive or develop secure disposal procedures. These should include removing references and configuration data, secure removal of data stored in the IAC Cyber Asset, especially security information such as encryption keys. The secure disposal of the IAC Cyber Asset may be required to prevent potential disclosure of data contained in the product that could not be removed as described.

### 7.3.8 PR.DS-4 – Adequate Capacity for Essential Function Availability

IAC essential functions take priority over all other functions and processes being performed in an IAC Segregated Environment. IAC Cyber Assets providing essential functions must be protected from outages caused by capacity being overwhelmed. This applies to the capacity of the IAC Cyber Asset's capabilities and services and of the capabilities and services provided by other IAC Cyber Assets (e.g. network capacity) within the IAC Security Zone or its IAC Security Conduits.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 7.3.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that capacity planning and analysis be included in IAC Cyber Asset essential function availability requirements.
2) The IAC Cybersecurity Plan requires that IAC Cyber Asset resources be prioritized for use by IAC essential functions over their use by security functions.

#### 7.3.8.2 Enhanced Profile Requirements

3) The IAC Cybersecurity Plan requires that audit record storage allocation and management consider IAC Cyber Asset capacity limitations to protect availability of essential functions provided or supported by the IAC Cyber Asset.

#### 7.3.8.2.1 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.3.9 PR.DS-5 – Data Leak Protection

Data leak is the accidental or unintentional unauthorized transfer of information, either by action or inaction, from inside company to an external destination. The data can be transferred physically or electronically. It can be caused by human error or by a flawed internal process. Unauthorized information disclosure about the IAC Cyber Environment can be used by adversaries to gain insight into its design, architecture, and security posture. The objective of Data Leak Protection is to ensure that those without a need to know about the IAC Cyber Environment are prevented from gaining access to that information through physical or electronic accidental or unintentional transfer.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); |

#### 7.3.9.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires confidentiality or non-disclosure agreements commensurate with the risk to IAC information are identified, documented, and regularly reviewed.
2) The IAC Cybersecurity Plan requires data protection requirements for the permanent removal of information from IAC Support Assets that are no longer needed, which are commensurate with the risk regardless of previous production use, for disposal, removal from the IAC Cyber Environment or any other reason.
3) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest all for an IAC Support Asset that are no longer needed.
4) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest in the possession of any worker that no longer is required to perform IAC Cyber Environment tasks (e.g. terminations, job transfers, retirements, etc.).
5) The IAC Cybersecurity Plan requires data protection requirements for the permanent removal of information from the possession of a worker who no longer is required to perform duties related to the IAC Cyber Environment.
6) The IAC Cybersecurity Plan requires that risk management processes identify risk to data-at-rest all for removable media used in an IAC Cyber Environment whether for support, maintenance, or production.
7) The IAC Cybersecurity Plan requires data protection requirements for the permanent removal of information from removable media that are no longer needed, which are commensurate with the risk regardless of previous production use.

#### 7.3.9.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.3.9.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.3.9.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to receive or develop secure disposal procedures. These should include removing references and configuration data, secure removal of data stored in IAC Support Assets or removable media, especially security information such as encryption keys. The secure disposal of the IAC Cyber Asset may be required to prevent potential disclosure of data contained in the product that could not be removed as described.

#### 7.3.9.5 Natural Gas Transmission Pipeline Supplemental Guidance

b) Special consideration should be given to data leak requirements regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 7.3.10 PR.DS-6 – IAC Cyber Integrity Protection

IAC Cyber Integrity Protection focuses on the support of IAC process integrity through protection of all data, including executables, used directly in or in support of the essential functions performed by the IAC Cyber Asset. The objective of IAC cyber Integrity protection is to provide direct support of the availability of the intended IAC essential functions as they were designed through the protection of the integrity of IAC software, firmware, and information.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); (5); |

#### 7.3.10.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the integrity of IAC security requirements specified in this standard is verified prior to an IAC Cyber Asset being placed into service in a production IAC Segregated Environment.
2) The IAC Cybersecurity Plan requires that the integrity of IAC security functions specified in this standard is verified after maintenance activities on an IAC Cyber Asset prior to being placed into service in a production IAC Segregated Environment.
3) The IAC Cybersecurity Plan requires that the IAC Cyber Asset’s executables be protected against unauthorized changes.
4) The IAC Cybersecurity Plan requires that any update (e.g. patches, new releases) to the IAC Cyber Asset’s executables are verified for authenticity and integrity prior to being placed into service in a production IAC Segregated Environment.

#### 7.3.10.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.3.10.3 Extended Profile Requirements

5) The IAC Cybersecurity Plan requires that the IAC Cyber Asset sets outputs to a predetermined state if normal operation of essential functions cannot be maintained.

#### 7.3.10.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to identify data requiring integrity protection and receive or develop secure update and security function integrity verification procedures. These should include testing procedures before and after any patches or upgrades.

### 7.3.11 PR.DS-7 – IAC Development and Test Zone Security.

Prioritization of IAC security activities and outcomes should always support the essential functions of the production processes they are designed to protect. The often less restrictive change control processes associated with IAC development and the dynamic quality of IAC test environments increases the risk to availability, integrity, and confidentiality of their IAC Cyber Assets. These more dynamic environments could cause unintended events and consequences related to development and testing activities to other IAC Cyber Assets in those environments.

IAC development and test environments could also be targeted by adversaries attempting to gain knowledge of potential vulnerabilities and attack vectors to compromise the production IAC Cyber Environment.

The objective of IAC development and test environment security is to protect the availability, integrity, and confidentiality of the IAC production systems they are intended to support.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.3.11.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that production IAC Segregated Environment do not contain any non-production IAC cyber assets nor non-production IAC zones.
2) The IAC Cybersecurity Plan requires that a non-production IAC Segregated Environment protect all data, including executables, that is or will be used in a production IAC Segregated Environment to the same extent as required by the production Segregated Environment.
3) The IAC Cybersecurity Plan requires that non-production IAC Segregated Environment user credentials be unique from production IAC Segregated Environment credentials.
4) The IAC Cybersecurity Plan requires that an IAC Security Conduit that connects a production IAC Security Zone with a non-production IAC Security Zone be secured as a production IAC Security Conduit.

#### 7.3.11.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.3.11.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.3.11.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to formally identify and implement security development and test processes and procedures.

b) Organizations should consider the risk of using production configuration data in a non-production security zone.

### 7.3.12 PR.DS-8 – IAC Cyber Asset Physical Integrity Protection.

IAC essential functions could be compromised through physical manipulation of IAC Cyber Assets.

The objective of IAC Cyber Asset Physical Integrity Protection is to support availability, integrity, and confidentiality of the IAC production systems through the verification of hardware integrity.

| | | |
|---|---|---|
| **P1:** None | **P2:** None | **P3:** (1); |

#### 7.3.12.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 7.3.12.2 Enhanced Profile Requirements

No Enhanced Profile specific requirements.

#### 7.3.12.3 Extended Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC Cyber Assets employ physical tamper detection mechanisms (e.g. tamper evident tape, physical access alerting).

#### 7.3.12.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to develop risk appropriate physical integrity detection processes and procedures.

b) All manufacturers, suppliers, system integrators, and operators of IAC Cyber Assets intended to be used in the ONG pipeline industry should consider sourcing hardware only from trusted sources.

c) ONG pipeline industry stakeholders should implement a 3rd party cyber risk assessment process for appropriately vetting their supply chains.

## 7.4 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 maintained and used to manage protection of information systems and assets.

### 7.4.1 PR.IP-1 – IAC Cyber Baseline Configuration.

A baseline configuration is the active permanent configuration of an IAC Segregated Environment. This is not to be confused with an API 1164 Baseline Profile. A baseline configuration exists for all implementations of API 1164 Profiles (Baseline, Enhanced, and Extended). Management of an IAC Cyber Environment's baseline configuration is a primary activity in any security program to ensure appropriate security controls are maintained across all IAC Cyber Assets.

Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for IAC Cyber Assets and IAC Cyber Systems or configuration items within those systems. Baseline configurations are a basis for future builds, releases, and/or changes to the IAC Cyber Environment. Baseline configurations include information about IAC Cyber Assets (e.g., standard software installed on workstations, servers, controllers, RTU's, flow-computers, smart sensors, and network components; current version numbers and patch information on operating systems and executables; and configuration settings/parameters), network topology, and the system architecture, including IAC security zone placement and configuration. Maintaining baseline configurations requires creating new baselines as IAC Cyber Assets and IAC Cyber systems change over time.

Without a comprehensive inventory of the baseline configuration for IAC Cyber Assets and IAC Cyber Systems, which comprise the IAC Cyber Environment, it is difficult to control and appropriately maintain the security measures implemented within an IAC Security Zone. The IAC baseline configuration documentation will be the basis upon which decisions will be made regarding changing security measures implemented in an IAC Security Zone.

The objective of the IAC Cyber Baseline Configuration is to develop, document, and maintain under configuration control, a current baseline configuration of the IAC Cyber Environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); | **P2:** (1); (2); (3); (4); (5); (6); (7); (12); (13); (14); (15); (16); | **P3:** (1); (2); (3); (4); (5); (6); (7); (12); (17); (18); (19); (20); (21); (22); (23); |

### 7.4.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration settings of IAC Cyber Assets be documented.
2) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration settings of IAC Cyber Environments be documented.
3) The IAC Cybersecurity Plan requires that consistent criteria be used to identify the IAC Cyber Asset capabilities that are required to support IAC essential functions (least functionality principle).
4) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes the IAC Cyber Asset capabilities that are required to support IAC essential functions (least functionality principle).
5) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes the interface characteristics, security requirements, and the nature of the information communicated for all ingress and egress communicates for IAC Segregated Environments.
6) The IAC Cybersecurity Plan requires that an IAC cyber baseline configuration for a non-production IAC Segregated Environment is maintained and managed separately from the production IAC Cyber Environment baseline configuration.
7) The IAC Cybersecurity Plan requires that IAC Cyber Asset's configuration be verified against the documented baseline configuration before it is placed into service in any production IAC Segregated Environment.
8) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes all IAC Internal Conduits between Baseline Profile IAC Security Zones.
9) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes all IAC External Conduits between Baseline Profile IAC Intermediate Zones and External Zones.
10) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes the security risks associated with Baseline Profile IAC Segregated Environments.
11) The IAC Cybersecurity Plan requires that the IAC cyber baseline configuration includes the security activities and outcomes of the customized controls implemented from the IAC Baseline Profile specified in this standard.

### 7.4.1.2 Enhanced Profile Requirements

12) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all external IAC transport services used.
13) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all IAC Internal Conduits between Enhanced Profile IAC Security Zones.
14) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all IAC External Conduits between Enhanced Profile IAC Intermediate Zones and External Zones.
15) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all IAC Security Conduits between Enhanced Profile IAC Security Zones and Baseline Profile Security Zones.
16) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes the security risks associated with Enhanced Profile IAC Segregated Environments.
17) The IAC Cybersecurity Plan requires that baseline configuration setting documentation includes the security activities and outcomes of the customized controls implemented from the IAC Enhanced Profile requirements specified in this standard.

#### 7.4.1.3 Extended Profile Requirements

18) The IAC Cybersecurity Plan requires that, at minimum, one previous IAC cyber baseline configuration is maintained to support baseline configuration rollback.
19) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all IAC Internal Conduits between Extended Profile IAC Security Zones.
20) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all conduits between Extended Profile IAC Security Zones and External Zones.
21) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all conduits between Extended Profile IAC Security Zone and Baseline Profile IAC Security Zones.
22) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration include all conduits between Extended Profile IAC Security Zone and Enhanced Profile IAC Security Zones.
23) The IAC Cybersecurity Plan requires that IAC cyber baseline configuration includes the security risks associated with Extended Profile Segregated Environments.
24) The IAC Cybersecurity Plan requires that baseline configuration setting documentation includes the security activities and outcomes of the customized controls implemented from the IAC Extended Profile requirements specified in this standard.

#### 7.4.1.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to develop baseline configuration documentation including architectural and as-built drawings.

### 7.4.2 PR.IP-2 – IAC System Development Life Cycle

The System Development Life Cycle (SDLC) is a multistep, iterative, structured, and methodical process used for technical and non-technical activities to manage decision-making progression to deliver a system with the expected level of quality. The systems-development life cycle is a standard set of processes often tailored to an individual company’s needs.

The objective of IAC System Development Life Cycle requirements is to provide a secure by design, defense-in-depth approach to designing, building, maintaining, and retiring IAC Cyber Assets.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.4.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC Cyber Assets be managed using a formal system development lifecycle process.
2) The IAC Cybersecurity Plan requires that IAC system development lifecycle processes incorporate IAC security considerations.
3) The IAC Cybersecurity Plan requires that IAC system development lifecycle processes define and documents IAC security roles and responsibilities throughout the system development life cycle.
4) The IAC Cybersecurity Plan requires that the IAC risk management process be integrated with the IAC system development life cycle activities.

#### 7.4.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.2.4 Supplemental Guidance

a) Organizations should consider only using IAC Cyber Asset manufacturers, suppliers, and system integrators who use a system development lifecycle process.

b) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to ensure the vendors’ system development lifecycle processes are compatible and meet the minimum-security requirements.

### 7.4.3 PR.IP-3 – IAC Configuration Change Control

A formal change control system, which includes testing, reviews, approvals, and evergreening of the baseline configuration documentation, is a foundational element to keeping an IAC Cyber Environment's baseline configuration current. It is a primary activity in any security program to ensure appropriate security controls are maintained across all IAC Cyber Assets. Changes to IAC Cyber Environment include modifications to hardware, software, or firmware components and configuration settings.

Configuration change controls for IAC Cyber Environments involve the systematic request, justification, creation, testing, review, and implementation of changes to the systems, including upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of IAC Cyber Assets, changes to configuration settings for IAC Cyber Assets, unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

Without a comprehensive inventory of the baseline configuration of an IAC Cyber Environment, it is difficult to control and appropriately maintain the security measures. The IAC baseline configuration documentation will be the basis upon which decisions will be made regarding changing security measures implemented in an IAC Security Zone. The objective of the IAC Cyber configuration change controls is to appropriately control and maintain the security measures implemented within an IAC Security Zone. The following control statements do not consider operational change control processes nor requirements.

| | | | | | |
|---|---|---|---|---|---|
| **P1:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); | **P2:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); | **P3:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); |

#### 7.4.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cyber configuration change control process be implemented to manage the IAC baseline configuration.
2) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process uses consistent criteria to define the types of changes to the IAC Cyber Environment that are in scope of the process.
3) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process documents configuration change decisions.
4) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process documents configuration changes that are intended to be temporary, including the duration the change is expected to be in effect.
5) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process tests configuration changes before being placed into service in a production IAC Segregated Environment, unless supported by a risk assessment.
6) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process reviews configuration changes, including test and risk assessment results, before implementation.
7) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes an API 1164 impact assessment for any IAC security zone or conduit for changes that could affect the baseline impact assessment.
8) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes cryptographic mechanisms, especially those that expire or otherwise require renewal are under configuration management.
9) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes an approval of the configuration change prior to implementation.
10) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes the key stakeholders in the change review and approval procedure.
11) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes the management who are accountable for the safety, integrity and reliability of the process controlled by the IAC Cyber Asset in the change review and approval procedure.
12) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes procedural or technical controls to rollback temporary changes when no longer required.

13) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process updates the baseline configuration inventory for permanent changes.
14) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes procedures to keep the as-built installed equipment connection and configuration documents, and network architectural diagrams, including IAC security zone membership lists current.
15) The IAC Cybersecurity Plan requires that the IAC risk management process be integrated with the IAC Cyber configuration change control process.
16) The IAC Cybersecurity Plan requires that the IAC Cyber configuration change control process includes emergency change procedure to address urgent changes needed to support essential function availability, integrity, and confidentiality.

#### 7.4.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.3.4 Supplemental Guidance

a) The IAC Cyber configuration change control process should follow separation of duty principles to avoid conflicts of interest.
b) The organization should consider leveraging any existing operational change control processes supporting or augmented by the above requirements.

#### 7.4.3.5 Hazardous Liquid Pipeline Supplemental Guidance

c) Title 49 CFR Part 195 Transportation of Hazardous Liquids by Pipeline, section 446 - Control room management, subsection (c) *Provide adequate information*, paragraph (2), requires a point-to-point verification between SCADA displays and related field equipment when field equipment is added or moved and when other changes that affect pipeline safety are made to field equipment or SCADA displays. Organizations should consider any cybersecurity relevant impacts when this regulatory requirement is employed.

#### 7.4.3.6 Natural Gas Transmission Pipeline Supplemental Guidance

d) Title 49 CFR Part 192 Transportation of Natural and Other Gas by Pipeline, section 631 – Control room management, subsection (c) *Provide adequate information*, paragraph (2) requires a point-to-point verification between SCADA displays and related field equipment when field equipment is added or moved and when other changes that affect pipeline safety are made to field equipment or SCADA displays. Organizations should consider any cybersecurity relevant impacts when this regulatory

### 7.4.4 PR.IP-4 – IAC Cyber Asset Backup and Restore

A business continuity plan identifies procedures for maintaining or re-establishing essential business operations while recovering from a significant disruption. The purpose of the business continuity plan is to provide a course of action to respond to the consequences of disasters, security failures, and the loss of service to a business.

IAC Cyber Asset and IAC Cyber System backup and restore processes are fundamental IAC Cybersecurity Program capabilities required to support business continuity. This includes specifying the frequency of backups, the retention duration of the backup data, and the frequency of restore capability testing, determining the amount of time/resources required for system restoration, location of backup files, including the environmental conditions under which they must be kept.

The objective of the IAC Cyber Asset Backup and Restore is to provide timely restoration of the availability and integrity of the IAC essential functions interrupted by data loss.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); |

#### 7.4.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires creation and maintenance of backup and restore procedures that support the business continuity plan’s objectives and risk targets.

2) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process uses consistent risk-based criteria for determining essential function(s) restoration timeframe targets.
3) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process do not adversely affect any essential functions of the IAC Cyber Asset, within the IAC Security zone or IAC Cyber Environment.
4) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process includes all data types necessary to create a complete backup that restores IAC Cyber Asset essential functions.
5) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process verify the integrity of backup data at the completion of the backup.
6) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process stores backup media in a safe and secure manner to protect its authenticity and availability when needed.
7) The IAC Cybersecurity Plan requires that IAC Cyber Asset backup and restore process specifies physical access limitations to the backup media commensurate with the data protection requirements of the data located on the backup media.

See Section 7.3.5 PR.DS-1 – IAC Data-at-Rest Protection (Inactive-Data) on page 56 above.

#### 7.4.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.4.4 Supplemental Guidance

a) IAC Cyber Asset backup and restore process's risk-based criteria for determining essential function(s) restoration timeframe targets should consider technology limitations (e.g. tape restore speed), the storage location(s) of backup media for immediate access for IAC Cyber essential function restoration versus off site storage to protect backup media from damage from localized environmental hazards (e.g. fire).

b) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to determine all the data types required to create a complete backup that will ensure the restoration of IAC Cyber Asset essential functions. The follow are some of the data types that should be considered: operation system, cryptographic data, applications (including middleware, such as OPC tunneling software), configuration data, database files, log files, electronic log book, unconventional file types including, but not limited to network equipment settings, control system controller settings (tuning parameters, set points, alarm levels), field instrumentation parameters, directory information and other files identified by the vendor.

### 7.4.5 PR.IP-5 – IAC Physical Operating Environment

Management of an IAC physical operation environment (attended or unattended) is a primary activity in any cyber security program to ensure appropriate security controls are maintained on all cyber assets across IAC Segregated Environments. Organizations should formally address the purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities and compliance requirements for its physical operating environment.

All technical infrastructure or specialized equipment utilized in providing cybersecurity should be physically protected against accident or attack and unauthorized physical access. Restricting physical access to authorized individuals helps ensure that IAC essential functions are available when needed.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 7.4.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Asset Physical Operating Environment requirements for IAC Cyber Assets and IAC Cyber Systems is documented.
2) The IAC Cybersecurity Plan requires that IAC Cyber Asset and IAC Cyber System manufacturers, suppliers, and system integrators provide documentation that details the security defense-in-depth

measures that are expected to be provided by the external environment to protect the IAC essential functions of IAC Cyber Solution.

3) The IAC Cybersecurity Plan requires that expected defense-in-depth measures to be provided by the external environment are designed, developed and implemented in collaboration with the personnel responsible for the physical security of the external environment in which the IAC Cyber Solution is deployed.
4) The IAC Cybersecurity Plan requires that risk-appropriate physical protection of the IAC Cyber Solution essential functions against natural disasters, malicious attack (e.g. vandalism) or accidents are designed, developed and implemented in collaboration with the personnel responsible for the physical security of the external environment in which the IAC Cyber Solution is deployed.

#### 7.4.5.2 Enhanced Profile Requirements

5) The IAC Cybersecurity Plan requires that IAC Cyber Asset shall be protected from power failures and other disruptions caused by failures in supporting utilities commensurate with the risk to IAC essential functions.
6) The IAC Cybersecurity Plan requires that IAC Cyber Asset telecommunications equipment and cabling be protected from interception, interference or damage commensurate with the risk to IAC essential functions.

#### 7.4.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.5.4 Supplemental Guidance

a) Procedures should address arrangements for non-cybersecurity personnel working around cybersecurity equipment to ensure the purpose of the equipment is on a need-to-know basis.

### 7.4.6 PR.IP-6 – Data Retention and Secure Disposal

The organization should have policies and procedures for the secure disposal of data stored on IAC equipment and associated media. This applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether the media is considered removable or not. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices.

The policies and procedure should include approved sanitization techniques of information system media, both digital and non-digital, prior to disposal or release for reuse. Sanitization is the process used to remove information from cyber asset media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that the destruction of the media is sometimes necessary when other methods cannot be applied to media requiring sanitization.

Organizations should use discretion on the employment of approved sanitization techniques and procedures for such media containing information or data. Destruction of hardware that has contained data protects against data theft and disclosure. Secure destruction can prevent losses due to cyber-espionage, accidental exposure, and abuse of trust or privilege.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 7.4.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC data, both digital and non-digital, are managed using information and document management processes.
2) The IAC Cybersecurity Plan requires that risk management processes identify risk to information and documents related to IAC Cyber Environment.
3) The IAC Cybersecurity Plan requires that information and document management processes address retention and destruction requirements commensurate with the risk identified.
4) The IAC Cybersecurity Plan requires that information and document retention and destruction requirements address IAC security and operation audit records.

#### 7.4.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.6.4 Supplemental Guidance

NIST Special Publication 800-88 – Guidelines for Media Sanitization*, revision 1*, December 2014 can assist an organization in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality.

### 7.4.7 PR.IP-7 – Continuous Improvement for Protection Processes

Cybersecurity performance should be monitored regularly and reported to stakeholders, providing relevant, accurate, and comprehensive assessment of IAC cybersecurity performance. The organization should have procedures for monitoring and reviewing the performance and effectiveness of their IAC Cybersecurity Program.

The continuous improvement of protection processes facilitates ongoing awareness of threats and vulnerabilities to support organizational risk management decisions and should be carried out at a defined frequency to generate appropriate risk responses.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 7.4.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that continuous improvement practices for protection processes are employed related to the IAC Security Program and IAC Security Plan reviews required in section 6.1 Governance (ID.GV) on page 25 above.
2) The IAC Cybersecurity Plan requires that continuous improvement practices for protection processes include reviewing lessons learned.

#### 7.4.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.4.8 PR.IP-8 – Sharing of Protection Technology Effectiveness

The organization should share appropriate types of information about the effectiveness of its protective measures with appropriate parties. Cybersecurity performance and the effectiveness of protection measures should be regularly reported to appropriate internal and external stakeholders to enable appropriate governance and timely collaboration on remediation or other actions.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); |

#### 7.4.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that protection technology effectiveness measurements are authorized, validated, and protected for confidentiality, integrity and availability from unauthorized access according to its information classification protection requirements.
2) The IAC Cybersecurity Plan requires that risk management processes identify risk to protection technology effectiveness measurements.

#### 7.4.8.2 Enhanced Profile Requirements

3) The IAC Cybersecurity Plan requires that access to protection technology effectiveness measurements is controlled using the need-to-know principle.
4) The IAC Cybersecurity Plan requires the identification of at least one authorized user to approve requests for access to protection technology effectiveness measurements.

5) The IAC Cybersecurity Plan requires that protection technology effectiveness measurements need-to-know considers external parties.
6) The IAC Cybersecurity Plan requires that external parties with access to protection technology effectiveness measurement are documented
7) The IAC Cybersecurity Plan requires that protection technology effectiveness measurements need-to-know considers responsible disclosure requirements regarding Supply Chain vulnerability management.

#### 7.4.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.8.4 Supplemental Guidance

a) Should consider protection technology effectiveness measurements need-to-know inclusion of appropriate information-sharing groups and collectives (e.g., cross-industry, cross-government, and cross-border groups).

#### 7.4.8.5 Natural Gas Transmission Pipeline Supplemental Guidance

b) Special consideration should be given to sharing of protection technology effectiveness regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 7.4.9 PR.IP-9 – Incident Response and Contingency Plans

Incident response and contingency planning for IAC Cyber Assets is an essential part of the overall IAC cybersecurity program. Contingency planning should address both system restoration and implementation of alternative mission/business processes when systems are compromised or exploited by cyber-threats. Contingency plans should specifically consider cybersecurity risks that could adversely affect IAC systems and assets.

It is important that organizations develop and implement a coordinated approach to incident response with cybersecurity functions. The IAC operator's incident response plan should be viewed as the first line of defense in an enterprise cybersecurity plan.

When developing the incident response plan, organizations should carefully consider the assumptions on which the incident response plan is based. Organizations should not assume a disaster caused by a cyber-incident will be limited to a single facility or a small geographic area.

IAC Incident response plans must accommodate disparate types of cyber threats to IAC Segregated Environments from both insiders and those external to the organization.

#### 7.4.9.1 Cyber Incident Response and Recovery Plan

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); |

##### 7.4.9.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires that a formal IAC Cyber Incident Response Plan be defined, which includes preparation, detection and analysis, containment, eradication, and recovery, to manage IAC cybersecurity risk associated with security incidents.
2) The IAC Cybersecurity Plan requires that risk management processes identify risk to the IAC Cyber Incident Response Plan associated with unauthorized disclosure and modification.
3) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan be classified and protected according to identified risk.
4) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan be approved by authorized personnel.
5) The IAC Cyber Incident Response Plan describes a high-level view for how the incident response capability fits into the overall organization.
6) The IAC Cyber Incident Response Plan considers unique requirements of the organization to appropriately address its mission, critical infrastructure role, size, structure, and IAC essential functions.
7) The IAC Cyber Incident Response Plan defines what is a reportable IAC cyber incident.

8) The IAC Cyber Incident Response Plan includes a communications plan.

9) The IAC Cyber Incident Response Plan identifies personnel with decision making authority and an escalation process.

10) The IAC Cyber Incident Response Plan defines the resources and management support needed to effectively maintain and mature an incident response capability.

### 7.4.9.1.2 Enhanced Profile Requirements

11) The IAC Cyber Incident Response Plan establishes and maintains a process that supports 24 hours a day cyber incident response. [*TSA*]

### 7.4.9.2 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.4.9.2.1 Supplemental Guidance

a) Consideration should be given to leveraging pipeline incident response processes.

### 7.4.9.3 IAC Cyber Contingency and Disaster Recovery Plan

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); |

### 7.4.9.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires that an IAC Cyber Contingency Response Plan be defined to manage IAC cybersecurity risk associated with disaster scenarios for maintaining the required level of operational continuity of IAC essential functions.

2) The IAC Cybersecurity Plan requires that the IAC Cyber Contingency Response Plan be approved by authorized personnel.

3) The IAC Cybersecurity Plan requires that copies of the IAC Cyber Contingency Response Plan be distributed to contingency personnel and organizational stakeholders.

4) The IAC Cybersecurity Plan requires that the IAC Cyber Contingency Response Plan be updated to address system and organizational changes.

5) The IAC Cybersecurity Plan requires that risk management processes identify risk to the IAC Cyber Contingency Response Plan associated with unauthorized disclosure and modification.

6) The IAC Cybersecurity Plan requires that the IAC Cyber Contingency Response Plan be information classified and protected according to identified risk.

7) The IAC Cybersecurity Plan requires that changes to the IAC Cyber Contingency Response Plan is communicated to contingency personnel and organizational stakeholders.

8) The IAC Cybersecurity Plan requires that IAC Cyber Contingency Response Plan activities be coordinated with IAC Cyber incident handling activities.

9) The IAC Cyber Contingency Response Plan identifies IAC Cyber essential functions and associated contingency requirements.

10) The IAC Cyber Contingency Response Plan documents contingency roles, responsibilities, and assigned individuals with contact information.

11) The IAC Cyber Contingency Response Plan identifies IAC Cyber Asset essential functions.

12) IAC Cyber Contingency Response Plan defines disaster recovery objectives, restoration priorities, and metrics (e.g. timing and capacity) to support IAC essential functions.

13) IAC Cyber Contingency Response Plan addresses eventual, full IAC restoration without deterioration of the IAC security safeguards originally planned and implemented.

### 7.4.9.3.2 Enhanced Profile Requirements

14) The IAC Cybersecurity Plan requires that the IAC Cyber contingency development be coordinated with other organization functions responsible for related plans.

#### 7.4.9.3.3 Extended Profile Requirements

15) The IAC Cybersecurity Plan requires that capacity planning be conducted to determine that the necessary capacity for IAC processing, telecommunications, and environmental support exists during contingency operations.

#### 7.4.9.3.4 Supplemental Guidance

a) No standalone IAC Cyber Contingency Response Plan is required. What is required is cyber risk to IAC essential functions is addressed in disaster scenarios for contingency plans. The IAC Cyber Contingency Response Plan is often developed and implemented as part of the overall business continuity planning process.

b) Special consideration should be given if a temporary reduction in the IAC cybersecurity posture is required during an event or event recovery period. Process should be in place to minimize the duration of the diminished posture to the shortest time practical and ensure a return to the IAC cybersecurity baseline state does occur.

### 7.4.10 PR.IP-10 – Response and Recovery Plans Testing

Organizations should undertake drills to test their incident response and recovery plans to ensure sufficient oversight, adequate capacity, and effective process capability for relevant cyber-events. Exercises should test communication channels, decision-making, and the technical capabilities of IAC Cyber Environment operators, as well as the cybersecurity incident responders.

These plans should address a range of scenarios, including severe but plausible scenarios (e.g., disruptive, destructive, corruptive) that could affect the organization's IAC essential functions. Organizations should plan and conduct routine response and recovery exercises and scenarios for the workforce to maintain awareness and effectiveness in responding to real world cyber-threats.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); (2); | **P3:** (1); (2); |

#### 7.4.10.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 7.4.10.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC Cyber Incident Response Plan exercises be conducted periodically. *[TSA*]

2) The IAC Cybersecurity Plan requires that IAC Cyber Contingency Response Plan be tested on a regular basis and updated, as necessary.

#### 7.4.10.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.10.4 Supplemental Guidance

a) While organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions from testing exercises, these risk-based decisions should be influenced by current threat and vulnerability assessments.

#### 7.4.10.5 Hazardous Liquid Pipeline Supplemental Guidance

b) Title 49 CFR Part 195 Transportation of Hazardous Liquids by Pipeline, section 446 - Control room management, , subsection (c) ) *Provide adequate information,* paragraph (4), requires that any backup SCADA systems are tested at least once each calendar year, but at intervals not to exceed 15 months. When applicable, organizations should consider coordinating or otherwise leveraging this regulatory requirement with other response and recovery testing activities.

#### 7.4.10.6 Natural Gas Transmission Pipeline Supplemental Guidance

c) Title 49 CFR Part 192 Transportation of Natural and Other Gas by Pipeline. Section 631 – Control room management, subsection (c) *Provide adequate information,* paragraph (4) requires any backup SCADA systems are tested at least once each calendar year, but at intervals not to exceed 15 months. When applicable, organizations should consider coordinating or otherwise leveraging this regulatory requirement with other response and recovery testing activities.

### 7.4.11 PR.IP-11 Human Resources Practices

An organization's human resources practices should have provisions that address IAC cybersecurity risk. An Employee with authorization to an IAC Cyber Environment may represent an insider threat, which is one of the most difficult to defend against.

The objective is to provide a level of assurance that the personnel with access to the IAC Cyber Environments are vetted to a level commensurate with the risk associated with the areas to which they have access.

| | | |
|---|---|---|
| **P1:** None | **P2:** (1); | **P3:** (1); |

#### 7.4.11.1 Baseline Profile Requirements

No Baseline Profile specific requirements

#### 7.4.11.2 Enhanced Profile Requirements

1) The IAC Cybersecurity Plan requires that, unless prohibited by law, all personnel, prior to access to the IAC Cyber Environment (both physical and cyber), are screened, including validation of their identity and background checks.

#### 7.4.11.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.11.4 Supplemental Guidance

d) Personnel screening processes should consider internal transfers of IAC cyber responsibilities to personnel who previously was not authorized to access the IAC Cyber Environment.

### 7.4.12 PR.IP-12 –Vulnerability Management Plan

Organizations should establish and maintain capabilities for ongoing vulnerability management programs to identify publicly known cyber vulnerabilities in the IAC Segregated Environment. The program should include technical vulnerability management procedures to monitor for and identify, assess, rank, and remediate cyber vulnerabilities in the IAC Segregated Environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 7.4.12.1 Baseline Profile Requirements

1) The IAC Cybersecurity Policy requires that a formal IAC Cyber Vulnerability Management Plan is defined to manage IAC cybersecurity risk associated identified vulnerabilities.
2) The IAC Cyber Vulnerability Management Plan uses the IAC Risk assessment process to determine appropriate risk responses to identified vulnerabilities.
3) The IAC Cyber Vulnerability Management Plan addresses the handling of vulnerabilities affecting the IAC Cyber Environment disclosed to the organization from outside sources (e.g. security researchers).
4) The IAC Cyber Vulnerability Management Plan addresses the handling of publicly disclosed vulnerabilities affecting the IAC Cyber Environment.
5) The IAC Cyber Vulnerability Management Plan addresses the use of automated vulnerability scanning tools on any production IAC Cyber Environment.
6) The IAC Cybersecurity Plan requires that IAC stakeholders responsible for the IAC vulnerability management are, at minimum, consulted and informed through formalized management-of-change processes on any physical or logical modification that could impact the cybersecurity of the IAC Cyber Environment.

#### 7.4.12.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.4.12.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 7.4.12.4 Supplemental Guidance

a) The organization should have a formal exception management process for vulnerabilities that cannot be mitigated due to business-related factors.

b) Organizations and cyber-incident response teams should have processes for receiving, reviewing, and responding to vulnerability disclosures. These practices help organizations and cyber-incident response teams make risk-informed decisions to mitigate, avoid, accept, or transfer the risks that flow from identified vulnerabilities. Establishing a coordinated vulnerability disclosure and handling process – and communicating the existence and scope of the process – help make ready an organizations to quickly detect, evaluate, prepare and respond to vulnerabilities disclosed to them by external sources, leading to mitigations that enhance the security, data privacy, and safety of IAC Cyber Environments.

## 7.5 Maintenance (PR.MA)

IAC Cyber Assets require proactive care and service to avoid or mitigate consequences of failure. Without a comprehensive risk-based review of maintenance personnel and maintenance tools for malicious activity and code, it is difficult to protect and appropriately maintain the integrity of an IAC Segregated Environment.

The objective of maintenance is to address the risk of failure to IAC Cyber Assets, while enforcing adequate controls to protect the IAC Segregated Environment from attack. The maintenance program extends security measures implemented in IAC Segregated Environments to maintenance personnel with local physical access or non-local access to IAC Cyber Assets and temporary equipment used as maintenance tools connecting to IAC Segregated Environment to perform maintenance activities.

### 7.5.1 PR.MA-1 – IAC Cyber Asset Maintenance and Repair

Maintenance activities introduce change to IAC Segregated Environments. In the event of a malfunction within the IAC Segregated Environment, maintenance records are a source for identifying tools, personnel, and change that has occurred. The information can assist in investigating the source and when the malfunction started, allowing organizations to determine appropriate steps to roll back the change.

Maintenance records document the work performed, when it was performed, how it was performed, by whom it was performed, and who has authorized the work.

IAC Cyber Systems require maintenance for efficient operations, documenting the maintenance extends security controls to ensure the maintenance is approved and performed by authorized personnel. The use of maintenance records is an important security control used as evidence to identify changes that have occurred in the event of malfunction or suspected malicious activity to the IAC Cyber System. Maintenance records detailing a time of change allows organizations to investigate the maintenance work performed and determine if the work performed introduced the activity in question.

| | | | | | |
|---|---|---|---|---|---|
| **P1:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); | **P2:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); | **P3:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); |

#### 7.5.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that maintenance of IAC Cyber Assets be documented, and records are reviewed periodically.

2) The IAC Cybersecurity Plan requires that IAC Cyber Asset maintenance records be retained according to their information classification and records retention schedule.

3) The IAC Cybersecurity Plan requires that maintenance of IAC Cyber Assets be performed according to manufacturer or vendor specifications and/or organizational requirements.

4) The IAC Cybersecurity Plan requires that maintenance of IAC Cyber Assets be approved by authorized personnel prior to being performed.

5) The IAC Cybersecurity Plan requires that potentially impacted security controls be verified that they are still functioning properly following maintenance and repair prior to the IAC Cyber Asset being placed into service in a production IAC Security Zone.

6) The IAC Cybersecurity Plan requires that IAC Cyber Asset maintenance tools be approved by authorized personnel.

7) The IAC Cybersecurity Plan requires that IAC Cyber Asset maintenance personnel be authorized prior to any maintenance performed.

8) The IAC Cybersecurity Plan requires that a list of authorized IAC Cyber Asset maintenance organizations and personnel be maintained.
9) The IAC Cybersecurity Plan requires that media containing diagnostic and test programs are tested for threats before the media are used on the IAC Cyber Asset.

#### 7.5.1.2 Enhanced Profile Requirements

10) The IAC Cybersecurity Plan requires that risk management processes identify risk to IAC Cyber Assets associated with unauthorized disclosure and modification of data prior to its removal from a company facility for off-site maintenance or repairs.
11) The IAC Cybersecurity Plan requires an approval by authorized personnel prior to the removal of an IAC Cyber Asset from a company facility for off-site maintenance or repairs.
12) The IAC Cybersecurity Plan requires that non-escorted personnel performing IAC Cyber Asset maintenance have required access authorizations.
13) The IAC Cybersecurity Plan requires that personnel with required access authorizations and technical oversight responsibility to supervise the maintenance activities of personnel who do not possess the required access authorizations.

#### 7.5.1.3 Extended Profile Requirements

14) The IAC Cybersecurity Plan requires that IAC Cyber Asset maintenance tools carried into a facility by maintenance personnel have been inspected for improper or unauthorized modifications prior to use.

### 7.5.2 PR.MA-2 – Nonlocal Maintenance

Nonlocal access is any human user access to an IAC Cyber Asset using network communications whether originating from inside an IAC Security Zone or an External Zone. Nonlocal access does not include individuals physically present and physically connected to an IAC Cyber Asset.

Proper authentication and logging of nonlocal access to IAC Cyber Assets should be deployed to detect user intrusion. Nonlocal access to IAC Cyber Assets is a potential attack vector for which malicious activity can be nonlocally activated to launch an attack on the IAC System.

The objective of Nonlocal Access Management is to mitigate the risk of unauthorized access through management of nonlocal connections using active approval chain(s), strong authenticators, session management, and log auditing.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); (14); (15); (16); (17); (18); |

#### 7.5.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that risk assessment processes identify risks associated with nonlocal maintenance and diagnostic capabilities for an IAC Cyber Asset or IAC Security Zone.
2) The IAC Cybersecurity Plan requires that nonlocal maintenance and diagnostic capabilities for an IAC Cyber Asset or IAC Security Zone are approved by authorized personnel.
3) The IAC Cybersecurity Plan requires that nonlocal maintenance of IAC Cyber Assets be documented, and records are reviewed periodically.
4) The IAC Cybersecurity Plan requires that IAC Cyber Asset nonlocal maintenance records be retained according to their information classification and records retention schedule.
5) The IAC Cybersecurity Plan requires that IAC Cyber Asset nonlocal maintenance and diagnostic services be performed from a Cyber Asset and Security Zone that implements a security capability comparable to the capability implemented on the IAC Cyber Asset and IAC Security Zone being serviced.
6) The IAC Cybersecurity Plan requires that nonlocal maintenance activities on IAC Cyber Assets are approved by authorized personnel.
7) The IAC Cybersecurity Plan requires that nonlocal maintenance activities on IAC Cyber Assets are logged.
8) The IAC Cybersecurity Plan requires that IAC Cyber Asset nonlocal maintenance and diagnostic tools for access to or use within an IAC Security Zone are approved by authorized personnel.

9) The IAC Cybersecurity Plan requires that a catalog of authorized IAC Cyber Asset nonlocal maintenance and diagnostic tools be maintained.
10) The IAC Cybersecurity Plan requires that strong authenticators be employed in the establishment of and IAC Cyber Asset nonlocal maintenance and diagnostic sessions.
11) The IAC Cybersecurity Plan requires that session and network connections be terminated when IAC Cyber Asset nonlocal maintenance is completed.
12) The IAC Cybersecurity Plan addresses the requirements for disabling IAC Cyber Asset nonlocal maintenance access account on consecutive failed login attempts.

#### 7.5.2.2 Enhanced Profile Requirements

13) The IAC Cybersecurity Plan requires that risk assessment processes identify risks associated with nonlocal maintenance and diagnostic tools used on an IAC Cyber Asset.
14) The IAC Cybersecurity Plan requires that failed login attempts to an IAC Cyber Asset nonlocal maintenance access account generate audit records.
15) The IAC Cybersecurity Plan requires that an IAC Cyber Asset nonlocal maintenance session terminates after a period of inactivity.

#### 7.5.2.3 Extended Profile Requirements

16) The IAC Cybersecurity Plan requires that a non-local human interactive session use two or more factors of authentication to access an IAC Intermediate Security zone.
17) The IAC Cybersecurity Plan requires that an IAC Intermediate Security Zone authenticate all human interactive sessions.
18) The IAC Cybersecurity Plan requires that the two/multi-factor authentication service be hardened and isolated from the External Zone.

## 7.6 Protective Technology (PR.PT)

Protective technologies include cybersecurity solutions which monitor and/or control access to IAC cybersecurity environments. The objective of Protective Technology is to minimize the attack surface and the adverse effects of attacks on the IAC Cyber Environment.

The IAC security zone determines the portfolio of protective technologies that should be applied. Properly implemented and maintained protection solutions may reduce the risk to IAC Cyber Assets to an acceptable level.

### 7.6.1 PR.PT-1 –Audit / log records

An organization should determine the need for and the extent of IAC system logging that is defined, documented, and implemented to assist in the continued operation of the IAC Cyber System. Auditing of these logs at defined frequencies maintains the availability, integrity, and confidentiality of the system. Using scripted and automatic logging functions, the IAC system can be audited for abnormalities or exceptions as part of incident detection refinement or incident response.

These log audits are helpful to detect and recover from cybersecurity incidents.

| | | | | | |
|---|---|---|---|---|---|
| **P1:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); | **P2:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); | **P3:** | (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); (12); (13); |

### 7.6.2 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a security audit capability exists for IAC Cyber Assets, IAC Security Zones, and IAC Security Zone Conduits including the generation, retention, review, and protection of IAC Security Events (IAC Audit Records).
2) The IAC Cybersecurity Plan requires that consistent criteria be used to define the types of security events required for auditing.
3) The IAC Cybersecurity Plan requires that security related configuration changes generate an IAC Security Event.
4) The IAC Cybersecurity Plan requires that IAC Audit Records contain information that establishes the type of event, the date and time of the event, the source of the event (originating device, software process or

human user account), the outcome of the event, and any access control accounts or the identity of any individuals or subjects associated with the event.

5) The IAC Cybersecurity Plan requires that consistent criteria be established to allocate and manage IAC Audit Record storage capacity.
6) The IAC Cybersecurity Plan requires that IAC Audit Record storage capacity be managed according to the risk and technical capability of the IAC Cyber Asset.
7) The IAC Cybersecurity Plan requires that an IAC audit processing failure does not cause the loss of IAC essential functions unless supported by a risk assessment.
8) The IAC Cybersecurity Plan requires that risk assessment processes identify risks associated with IAC Audit Records.
9) The IAC Cybersecurity Plan requires that all IAC Audit Records be authorized, validated, and protected for confidentiality, integrity, and availability from unauthorized access according to its information classification protection requirements.
10) The IAC Cybersecurity Plan requires that IAC Audit Records be information classified by their protection requirements.
11) The IAC Cybersecurity Plan requires that consistent criteria be established to determine the frequency of periodic reviews of IAC Audit Records.
12) The IAC Cybersecurity Plan requires that IAC Cyber Asset risk be a criterion used to determine the frequency of periodic reviews of IAC Audit Records.

#### 7.6.2.1 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.6.2.2 Extended Profile Requirements

13) The IAC Cybersecurity Plan requires that personnel be alerted in the event of an IAC Audit Event processing failure.

#### 7.6.2.3 Supplemental Guidance

a) Pipeline IAC Cyber Environments cover a wide geographic area with decentralized sites, some of which have limited network connectivity or network bandwidth. Consideration should be given to log size limitations and log collection frequency to ensure they do not impact IAC essential functions.

### 7.6.3 PR.PT-2 –Removable Media

Removable media is a form of data storage that can be inserted and removed from a system.

The use of removable media may increase the level of cybersecurity risk to an IAC cyber system beyond acceptable levels.

Controlling the use of removable media may decrease the level of potential data integrity issues within the IAC Cyber Asset or IAC Cyber System.

The protection of the IAC system from malicious and unwanted code is the prime objective of restricting the use of any removable media.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); | **P2:** (1); (2); (3); (4); (5); (6); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 7.6.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that any removable media, regardless of content or purpose is tested for threats before the media is used on or by an IAC Cyber Asset whether in a production, test, or development environment.
2) The IAC Cybersecurity Plan requires that any removable media, regardless of content or purpose is approved by authorized personnel before the media is used on or by an IAC Cyber Asset whether in a production, test, or development environment.
3) The IAC Cybersecurity Plan requires that any removable media, regardless of content or purpose is tagged, labeled, or otherwise marked as approved by authorized personnel before the media is used on or by an IAC Cyber Asset whether in a production, test, or development environment.

4) The IAC Cybersecurity Plan requires that any modification, update, or addition of content to IAC authorized removable media nullifies its authorization for use on or by an IAC Cyber Asset.
5) The IAC Cybersecurity Plan requires that CD and DVD media be treated as removable.

#### 7.6.3.2 Enhanced Profile Requirements

6) The IAC Cybersecurity Plan requires that processes exist to protect any removable media from modification after its authorization for use on or by an IAC Cyber Asset.

#### 7.6.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 7.6.4 PR.PT-3 – Least Functionality Principle

The Least Functionality Principle establishes that IAC Cyber Assets are configured to provide only the functions and services required to perform the tasks defined by its role in the automation solution. It also specifies the prohibition, restriction or removal of all functions and services not required.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); (3); |

#### 7.6.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC Cyber Asset be configured according to the baseline configuration to provide only those capabilities that are required to support IAC essential functions and all other capabilities are disabled.
2) The IAC Cybersecurity Plan requires that management-of-change processes verify that only the capabilities that are required to support IAC essential functions are enabled and all others are disabled prior to an IAC Cyber Asset being placed into service in any production IAC Security Zone.

#### 7.6.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.6.4.3 Extended Profile Requirements

3) The IAC Cybersecurity Plan requires that periodic reviews are conducted to validate that IAC Cyber Assets are configured according to the baseline configuration to provide only those capabilities that are required to support IAC essential functions and all other capabilities are disabled.

### 7.6.5 PR.PT-4 – IAC Network and Communications Protection

Protecting IAC networks and communications is critical to the availability, integrity, and data protection of IAC essential functions performed in IAC Segregated Environments. Consideration should be given to security practices that recommended by the IAC Cyber Asset manufacturers, suppliers, and system integrators when implementing the requirements below. That, along with management (identification and limits) of data types and communication paths will help maintain effective operations.

Persistent monitoring and defined limits for communications along with data norms in both direction and value will deliver the highest level of availability while retaining the integrity of these communications.

NOTE Refer to Section 5.4.1.4 IAC Zone and Conduit Taxonomy on page 19 above to better understand Security Zone and Security Conduit types and their relationships.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); (9); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (10); (11); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); (9); (11); (12); |

#### 7.6.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that communications at IAC Segregated Environment boundaries be monitored and controlled.
2) The IAC Cybersecurity Plan requires that all IAC Cyber Assets shall inherit the API 1164 Profile requirements from the IAC Security Zone or IAC Security Conduit to which it is a member.
3) The IAC Cybersecurity Plan requires that IAC Security Zones only communicate outside the security perimeter through an IAC Security Conduit.

4) The IAC Cybersecurity Plan requires that an IAC Cyber Asset, which is required to communicate with an External Security Zone for data or services, must only do so through an IAC External Conduit.
5) The IAC Cybersecurity Plan requires that an IAC External Conduits only connect to External Zones and IAC Intermediate Zones.
6) The IAC Cybersecurity Plan requires that an IAC Intermediate Zone must only communicate through an IAC External Conduit or an IAC Intermediate Conduit.
7) The IAC Cybersecurity Plan requires that IAC Intermediate Conduits only connect to IAC Intermediate Zones and IAC Internal Zones.
8) The IAC Cybersecurity Plan requires that an IAC Internal Zone must only communicate through an IAC Intermediate Conduit or an IAC Internal Conduit.
9) The IAC Cybersecurity Plan requires that an IAC Security Conduit deny all ingress and egress communications with an IAC Intermediate Security Zone that are not identified in the Baseline Configuration as required to support IAC essential functions.

#### 7.6.5.2 Enhanced Profile Requirements

10) The IAC Cybersecurity Plan requires that an IAC Security Zone Conduit that connects an Enhanced Profile IAC Security Zone with another IAC Security Zone, regardless of API 1164 Profile level, explicitly deny all egress and ingress communications that are not identified in the Baseline Configuration as are required to support IAC essential functions.
11) The IAC Cybersecurity Plan requires that IAC Security Conduits, which use external IAC transport services, address the risk to availability, integrity, and data security of IAC essential functions from threats, including man-in-the-middle (MitM) and man-on-the-side (MotS) attacks.

#### 7.6.5.3 Extended Profile Requirements

12) The IAC Cybersecurity Plan requires that an IAC Security Zone Conduit that connects an Extended Profile IAC Security Zone with another IAC Security Zone, regardless of API 1164 Profile level, explicitly deny all egress and ingress communications that are not identified in the Baseline Configuration as are required to support IAC essential functions.

### 7.6.6 PR.PT-5 – Situational Resilience

Situational resilience is the capability of an IAC Cyber Asset to perform IAC essential functions during a cyber event.

The IAC system should be configured according to manufacturer recommendations and commonly accepted industry practices to maintain continued operations in the event of a cyber incident. By employing mechanisms such as redundancy, fail safes, load balancing, and the like, the IAC system can achieve the level of operation during normal and adverse situations set forth by the business' operational needs.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); (5); (6); |

#### 7.6.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC Cyber Asset availability and resiliency requirements are defined.
2) The IAC Cybersecurity Plan requires that an IAC Security Zone and the IAC Security Zone Conduits used by the Zone are considered collectively when defining availability and resiliency requirements.
3) The IAC Cybersecurity Plan requires that IAC Security Zone impact assessment be considered when defining IAC Cyber Asset availability and resiliency requirements.
4) The IAC Cybersecurity Plan addresses priority-of-service provisions for any services provided by or facilities shared with 3rd parties in accordance with availability and resiliency requirements (e.g. Organization gets priority use of shared office space within colocation data center during business continuity event or test).

#### 7.6.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 7.6.6.3 Extended Profile Requirements

5) The IAC Cybersecurity Plan requires alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
6) The IAC Cybersecurity Plan requires primary and alternate telecommunications service providers to have contingency plans.

# 8 ONG IAC Cybersecurity Profile Requirements - Detect (DE)

The Detect function addresses the activities associated with the timely detection and identification of the occurrence of a cybersecurity event. The elements in the Detect function is critical to the successful implementation of the Framework as Response and Recovery activities rely on its effective facility. The target profile outcome Categories and Subcategories within this function are detailed below.

## 8.1 Anomalies and Events (DE.AE)

Anomaly and Event Detection sets the groundwork for an effective Detect Function by citing the need for understanding of baseline network operations and data flows within the IAC Cyber Environment. It calls for the establishment of event thresholds and better understanding of the impacts when those thresholds are exceeded. Robust Anomaly and Event Detection supports IAC system monitoring, response, and recovery activities.

### 8.1.1 DE.AE-1 – Dataflows and Network Operation Baselines

Baseline measurements of dataflows and overall network behavior record normal (typical) movement of information through the IAC Cyber Environment. These measurements are used to identify indications of abnormal events or data flows. Organizations should seek to define baseline behavior for the IAC Cyber Environment to facilitate further investigation and response.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 8.1.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that human and machine expected egress and ingress data flows that traverse an IAC Security Conduit are included in the IAC Cyber Baseline Configuration.

#### 8.1.1.2 Enhanced Profile Requirements

2) The IAC Cybersecurity Plan requires that human and machine expected data flows within an IAC Security Zone are included in the IAC Cyber Baseline Configuration.

#### 8.1.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.1.1.4 Supplemental Guidance

a) Organizations should work with their IAC Cyber Asset manufacturers, suppliers, and system integrators to develop baseline configuration documentation including expected data flows and network operations.

### 8.1.2 DE.AE-2 – Security Event Detection and Analysis

Dataflows and network behavior that falls outside of the identified baseline may indicate a security event. Further investigation will be required to rule out compromise or drive response action. Organizations should establish means (manual or automatic) to detect events that are departures from baseline and provide for detailed analysis to understand the nature of the event and identify actions required.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); (3); |

#### 8.1.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that audit record anomalies be analyzed to determine that the classification of the anomalies are a true indication of an incident.
2) The IAC Cybersecurity Plan requires that security events be analyzed to understand potential attack targets and methods of the IAC Cyber Asset(s) in which it was detected.

#### 8.1.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.1.2.3 Extended Profile Requirements

3) The IAC Cybersecurity Plan requires that automated mechanisms be implemented to support analysis of event logs to identify attack targets and methods.

### 8.1.3 DE.AE-3 – Event data Aggregation and Correlation

Data aggregation and correlation is the gathering and association of various network or system information that when aligned provide a view that may not be visible independently. Such an approach can be vital to creating context about abnormal events to allow for more complete analysis. Organizations will benefit from performing data aggregation and correlation from a variety of sources to support investigation activities.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 8.1.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that cybersecurity event data collected from multiple sources including assessments and monitoring are correlated and analyzed.

#### 8.1.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.1.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.1.3.4 Supplemental Guidance

a) Within the context of DE.AE-3 the term correlation does not imply nor assume the use of any automation, including a Security Information and Event Management (SIEM) system.

b) SIEM tools automate the process of collecting, aggregating, and correlating event data from multiple cyber assets. It is often the best, and sometimes the only, practical way to analyze medium to large sets of data in a timely way. Consideration should be given to aggregation and correlation automation solutions when manual means are not sufficient or practical.

c) Pipeline IAC Cyber Environments cover a wide geographic area with decentralized sites, some of which have limited network connectivity or network bandwidth. Consideration should be given to the methods available to collect event data to ensure it does not impact IAC essential functions.

d) Pipeline systems can pass through multiple jurisdictions with varying regulatory requirements, including requirements for monitoring, privacy, time synchronization, and safety. Consideration should be given to all applicable regulatory requirements when developing monitoring and logging processes, including event data collection processes that cross jurisdictional boundaries.

### 8.1.4 DE.AE-4 – Event Impact

The impact of a cybersecurity event can reach a wide scope of business elements, both internal and external to an organization. The impact scope can be extended beyond the organization depending on the location of the event within the supply chain. Organizations should evaluate events using the same scope and criteria so that impacts are understood, and appropriate responses can be determined.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 8.1.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that IAC cybersecurity event data be analyzed to determine the potential impact to IAC essential functions.

2) The IAC Cybersecurity Plan requires that consistent criteria be used to measure impact of IAC cyber events.

3) The IAC Cybersecurity Plan requires that the IAC 1164 Impact Assessment be used to determine the potential impact to the IAC Cyber Environment.

#### 8.1.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.1.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.1.5 DE.AE-5 – Incident Thresholds

Incident Thresholds define the boundary between what the organization considers a significant versus an insignificant cyber event. Exceeding incident threshold parameters should drive defined and coordinated response actions, which may include automated functions. The objective of Incident Thresholds is to determine whether a response is required based on cyber security event criteria being exceeded.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 8.1.5.1 Baseline Profile Requirements

1) IAC Cyber Incident Response Plan defines consistent criteria for determining the alert thresholds for an IAC cyber incident.
2) IAC Cyber Incident Response Plan includes incident handling processes for determining the alert thresholds for the potential presence of an IAC cyber incident.

#### 8.1.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.1.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

## 8.2 Security Continuous Monitoring (DE.CM)

Monitoring the IAC Cyber Environment for cybersecurity events is a fundamental element of an IAC security program. To be effective the monitoring should be done at discrete intervals and should verify the effectiveness of the IAC Cybersecurity Program's protective measures.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); (8); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); |

#### 8.2.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cybersecurity monitoring program be implemented to detect security related events.
2) The IAC Cybersecurity Plan requires that consistent criteria be used to determine which IAC security events and activities will be monitored and the frequency of that monitoring.
3) The IAC Cybersecurity Plan requires that a risk assessment process be used to influence which IAC security events and activities that will be monitored and the frequency of that monitoring.
4) The IAC Cybersecurity Plan requires that the IAC 1164 Impact Assessment be used to influence which IAC security events and activities that will be monitored and the frequency of the monitoring.
5) The IAC Cybersecurity Plan requires that the IAC Cybersecurity monitoring program includes IAC Cyber Assets.
6) The IAC Cybersecurity Plan requires that all IAC Cyber Assets within an IAC Segregated Environment are set to the same level of security events, activities, and frequency as that of the of the highest IAC Cyber Asset within the IAC Segregated Environment.
7) The IAC Cybersecurity Plan requires that risk management processes identify risk associated with unauthorized disclosure of and modification to IAC Cybersecurity monitoring program documented artifacts (e.g. detected event logs and vulnerability scan results).
8) The IAC Cybersecurity Plan requires that the IAC Cybersecurity monitoring program documented artifacts are classified and protected according to identified risk.

#### 8.2.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.2.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.2.1.4 Supplemental Guidance

a) In the context of this Security Continuous Monitoring category and its subsequent subcategories, the term “continuous” is to be interpreted to mean at discrete intervals in time. The degree of automated real-time monitoring and alerting should be made as a risk appropriate decision.

### 8.2.2 DE.CM-1 – Continuous Network Monitoring

Network monitoring involves the collection, analysis, and escalation of indications and warnings to detect and respond to anomalous network behavior. Implementing a risk-based network monitoring strategy helps to ensure the availability, integrity, and confidentially of the IAC cyber environment by detecting and responding to anomalous network behavior in a timely manner.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); (2); | **P3:** (1); (2); (3); |

#### 8.2.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that an IAC Cybersecurity monitoring program include ingress and egress for IAC Security Conduits.

#### 8.2.2.2 Enhanced Profile Requirements

2) The IAC Cybersecurity Plan requires that an IAC Cybersecurity monitoring program includes communications within an IAC Intermediate Security Zone.

#### 8.2.2.3 Extended Profile Requirements

3) The IAC Cybersecurity Plan requires that an IAC Cybersecurity monitoring program includes communications within an API 1164 Extended Profile IAC Security Zone.

### 8.2.3 DE.CM-2 –Physical Environment Monitoring

Physical monitoring involves the collection, analysis, and escalation of indications and warnings to detect and respond to anomalous physical behavior. Physical monitoring employs the use of multiple layers of interdependent systems that can include CCTV surveillance, security guards, protective barriers, locks, access control, access logs, perimeter intrusion detection, deterrent systems, tamper evident seals, fire protection, and other systems designed to protect persons and property. Physical protection of cyber asset is critical to the electronic security of that asset. Developing and implementing a risk-based physical monitoring strategy helps to ensure anomalous physical behavior is detected and responded to in a timely manner to ensure the availability, integrity, and confidentially of the IAC cyber environment.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 8.2.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cybersecurity monitoring program coordinates with the organization’s physical security function for physical security events that are used for IAC Cyber Environment monitoring.

#### 8.2.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.2.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.2.3.4 Supplemental Guidance

Organizations should strongly consider implementing controls to detect physical access to sites, which support critical IAC essential functions. Examples of such controls may include, but are not limited to, video monitoring, gate log events, locks, tamper evident seals, and door switches.

### 8.2.4 DE.CM-3 – Personnel Activity Monitoring

Monitoring the physical and cyber activities of personnel helps to ensure the availability, integrity, and confidentially of the IAC cyber environment. Personnel activities that cause degradation of the system either intentionally or unintentionally can be identified and addressed in a timely manner via real-time monitoring or via timely log review. Monitoring activities should support the company's risk profiles and should be implemented in those areas where technically feasible.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 8.2.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cybersecurity monitoring program includes personnel activity related to interacting with IAC Cyber Assets.
2) The IAC Cybersecurity Plan requires that the IAC Cybersecurity monitoring program considers privacy and civil liberties issues through the collaboration with the organization's Legal, Compliance, and Human Resource Functions.

#### 8.2.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.2.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.2.5 DE.CM-4 –Malware Detection

Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code has been known to adversely affect the availability, integrity, and confidentially of the IAC cyber environment.

Malicious code protection mechanisms should be implemented to support the organization's risk profiles and may include anti-virus signature definitions, reputation-based technologies, or other technologies. Such technologies not only identify and quarantine such code but may also limit or eliminate the effects of malicious code. Organizations should determine their response to the detection of malicious code during periodic scans, detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

| | | |
|---|---|---|
| **P1** (1); (2); (3); (4); (5); (6); | **P2** (1); (2); (3); (4); (5); (6); | **P3** (1); (2); (3); (4); (5); (6); |

#### 8.2.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a risk assessment process be used to determine the risk of an IAC Segregated Environment being exposed to malware whether a production, test, or development environment.
2) The IAC Cybersecurity Plan requires that the API 1164 IAC Impact Assessment be used in risk assessment processes for determining risk from malware.
3) The IAC Cybersecurity Plan requires that malware detection mechanisms be employed according to manufacturers', suppliers', and system integrators' recommended practices.
4) The IAC Cybersecurity Plan requires that malware detection mechanisms be updated according to manufacturers', suppliers', and system integrators' recommended practices.
5) The IAC Cybersecurity monitoring program includes malware detection mechanisms that are employed according to the technical capability of the IAC Cyber Asset and the risk to its essential functions.
6) The IAC Cybersecurity monitoring program includes malware detection mechanisms that are employed within the IAC Security Zone according to the risk to its IAC Cyber Asset(s)' essential functions.

#### 8.2.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.2.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.2.5.4 Supplemental Guidance

a) Periodic distribution of malware signature files can present a challenge to IAC Cyber Environments with limited network connectivity or network bandwidth. Consideration should be given to the methods available to update malware detection solutions.

b) Controlling software installation on a station HMI or other IAC Cyber Asset can be difficult without a centrally managed user roles and accounts. While malware detection is important in IAC Cyber Assets there does exist the possibility of false positives. Special consideration should be given to baselining and validating malware detection solutions prior to deployment withing a production IAC Cyber Environment. Consideration should be given to validating updates to malware detection solutions, both to the core software and to any signature or other malware identifying attribute updates.

### 8.2.6 DE.CM-5 – Mobile Code Detection

Mobile code in this context is code that is built upon a base executable that runs the code indirectly. The ability to have the base executable compiled for multiple platforms allows the code itself to be moved to multiple platforms, thus making it mobile. This makes it harder to control its execution because the base code is often approved to run but the code it is running may not be considered an executable by traditional security tools. Some examples of this technology are Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript

Unauthorized mobile code can cause significant issues to the IAC cyber environment and usage restrictions and implementation guidance should be applied to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and device. Mobile code detection procedures should be established and respond procedures implemented to mitigate the risk to the IAC cyber environment.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5 | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 8.2.6.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a risk assessment process is used to determine the risk to an IAC Security Zone associated with the use of mobile code within an IAC Cyber Environment whether in a production, test, or development environment.

2) The IAC Cybersecurity Plan requires that the API 1164 Impact Assessment be used in risk assessment processes for determining risk associated with mobile code.

3) The IAC Cybersecurity Plan requires that any use of mobile code within an IAC Cyber Environment is approved by authorized personnel before its use on or by an IAC Cyber Asset whether in a production, test, or development environment.

4) The IAC Cybersecurity Plan requires that mobile code be only used in an IAC Cyber Environment according to manufacturers', suppliers', and system integrators' recommended practices whether in a production, test, or development environment.

5) The IAC Cybersecurity monitoring program includes the monitoring of mobile code execution within an IAC Cyber Environment whether in a production, test, or development environment.

#### 8.2.6.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.2.6.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.2.6.4 Supplemental Guidance

a) Mobile code execution platforms should be under consideration to be removed or disabled when implementing the least-functionality principle within the IAC Cyber Environment.

### 8.2.7 DE.CM-6 – External Service Provider Monitoring

External service providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. External services providers may have personnel working either physically at the organization's facilities or through a network connection using credentials, badges, or information system privileges, which allows them access to IAC Cyber Assets. External service providers' access to IAC Cyber Assets, both physical and logical, should be risk assessed and additional monitoring procedures implemented for those providers who pose a risk higher than your risk tolerance.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

### 8.2.7.1 Baseline Profile Requirements

1) The IAC Cybersecurity monitoring program includes External Service Provider activities when providing services locally to the IAC Cyber Environment.
2) The IAC Cybersecurity monitoring program includes External Service Providers' activities when providing services when not connected locally to the IAC Cyber Environment.

### 8.2.7.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 8.2.7.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.2.8 DE.CM-7 – Monitoring for Unauthorized Activity

Unauthorized activity, devices, or software represents a significant security risk to the IAC Cyber Environment and can represent intent to gain unauthorized access to the IAC Cyber Environment. Methods, whether manual, automated, or both, should be deployed to effectively monitor and detect such activity.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

### 8.2.8.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a risk assessment process is used to determine the risk to an IAC Security Zone associated with unauthorized personnel interactions, connections, devices, and software within an IAC Cyber Environment whether in a production, test, or development environment.
2) The IAC Cybersecurity Plan requires that the API 1164 Impact Assessment be used in risk assessment processes for determining risk associated with unauthorized activity.
3) The IAC Cybersecurity monitoring program includes the monitoring for unauthorized personnel interactions, connections, devices, and software within an IAC Cyber Environment whether in a production, test, or development environment.

### 8.2.8.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 8.2.8.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.2.8.4 Supplemental Guidance

a) Shared or functional user accounts are often used in IAC Cyber Environments for a variety of reasons. These types of accounts violate the security principle of nonrepudiation and can violate the principle of least-functionality. These types of user accounts can make it exceedingly difficult to track what activity is authorized versus unauthorized. Organizations should strongly consider implementing alternate authentication and authorization methods other than shared or functional user accounts.

### 8.2.9 DE.CM-8 – Vulnerability Detection

Organizations determine the frequency and comprehensiveness of vulnerability scans based on the criticality of their IAC systems and their IAC Cyber Assets. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Vulnerabilities identified should be risk assessed and risk prioritized as to their remediation.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5); (6); (7); | **P2:** (1); (2); (3); (4); (5); (6); (7); (8); | **P3:** (1); (2); (3); (4); (5); (6); (7); (8); |

#### 8.2.9.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that a risk assessment process be used to determine the risk to an IAC Security Zone's essential functions associated with the use of automated vulnerability detection technologies within a production IAC Cyber Environment.
2) The IAC Cybersecurity Plan requires that the API 1164 Impact Assessment be used in risk assessment processes for determining risk associated with automated vulnerability detectors.
3) The IAC Cybersecurity Plan requires that any use of an automated vulnerability detector within a production IAC Cyber Environment is approved by authorized personnel before its use.
4) The IAC Cybersecurity Plan requires that automated vulnerability detectors be only used in a production IAC Cyber Environment according to manufacturers', suppliers', and system integrators' recommended practices.
5) The IAC Cybersecurity Plan requires that a risk assessment process be used to determine the risk to vulnerability lists.
6) The IAC Cybersecurity Plan requires that a risk assessment be performed on any automated vulnerability identification method to determine risk to IAC essential functions before being employed on or within an active production IAC Segregated Environment.
7) The IAC Cybersecurity Plan requires that the automated vulnerability identification risk assessment recommendations be reviewed and approved by a formally authorized member from both the IAC Operations and the ICS Cybersecurity organizations prior to being implemented and employed.

#### 8.2.9.2 Enhanced Profile Requirements

8) The IAC Cybersecurity monitoring program includes automated vulnerability detectors in development or test IAC Cyber Environments that are in support of production IAC Cyber Environments with an API 1164 Impact Rating of I2-Medium or higher.

#### 8.2.9.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.2.9.4 Supplemental Guidance

a) The deterministic nature of an IAC network operates under the assumption that the network traffic is of a known type and within a known volume. Performing automated vulnerability scans on this type of environment can put challenges on this operating assumption. The result can be that the availability and integrity of some IAC essential functions are impacted given the increased traffic. Special consideration should be given to throttling the vulnerability scanner's rate, so the additional network traffic does not impact the IAC essential functions of a production network.

## 8.3 Detection Processes (DE.DP)

The objective of Detection Processes is to ensure proper ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The IAC Cybersecurity Plan requires that detection processes and procedures are maintained and tested.

### 8.3.1 DE.DP-1 – Detection Processes Roles and Responsibilities

Roles and responsibilities define accountability for operation, maintenance, and testing of detection processes defined by the IAC Cybersecurity Plan. It is important to define roles and responsibilities to ensure effective information security, identify weaknesses and deficiencies early in the development process, provide essential information needed to make risk-based decisions, and ensure compliance with the IAC Cybersecurity Plan.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 8.3.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the roles and responsibilities for detection processes and procedures with the IAC Cybersecurity monitoring program is defined.
2) The IAC Cybersecurity Plan requires that the roles and responsibilities for the IAC Cybersecurity monitoring program are updated to address changes to the organization or IAC Cyber Environment.
3) The IAC Cybersecurity Plan requires that roles and responsibilities for the IAC Cybersecurity monitoring program are communicated to organizational stakeholders.

#### 8.3.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.3.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.3.2 DE.DP-2 – Compliance with Detection Requirements

Compliance ensures that detection functions meet all applicable requirements and ensure compliance with vulnerability mitigation procedures to maintain the security posture of the IAC Cyber Environment during the entire life cycle.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 8.3.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that periodic reviews be conducted to validate that the IAC Cybersecurity monitoring program detection mechanisms are configured according to the baseline configuration.
2) The IAC Cybersecurity Plan requires that periodic reviews be conducted to validate that the IAC Cybersecurity monitoring program processes and activities are executed according to the requirements of the IAC Cybersecurity Plan.

#### 8.3.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.3.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.3.2.4 Supplemental Guidance

a) Consider additional requirements, where applicable, from the following: TSA, PHMSA, CFATS, and CFRs.

### 8.3.3 DE.DP-3 – Testing of Detection Processes

Testing will ensure that detection processes are designed to achieve the control objectives of the IAC Cybersecurity Plan. Testing is an important part of maintaining the security posture of the IAC Cyber Environment to minimize the risk of flaws or discrepancies in the detection process that may lead to vulnerabilities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 8.3.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that periodic testing of the design effectiveness of technical controls is conducted to assess the IAC Cybersecurity monitoring program detection mechanisms. (i.e. The technical security controls in place are designed sufficiently to achieve the control objectives).
2) The IAC Cybersecurity Plan requires that periodic testing of the operating effectiveness of technical controls is conducted to assess the IAC Cybersecurity monitoring program detection mechanisms (i.e. The technical security controls in place are operated sufficiently to achieve the control objectives).

3) The IAC Cybersecurity Plan requires that periodic testing of the design effectiveness of procedural controls is conducted to assess the IAC Cybersecurity monitoring program detection mechanisms. (i.e. The procedural security controls in place are designed sufficiently to achieve the control objectives).
4) The IAC Cybersecurity Plan requires that periodic testing of the operating effectiveness of procedural controls is conducted to assess the IAC Cybersecurity monitoring program detection mechanisms. (i.e. The procedural security controls are operating as designed and the persons performing control activities have sufficient authority and competence to perform them effectively to achieve the control objectives).

#### 8.3.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.3.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 8.3.4 DE.DP-4 – Communication of Event Detection Information

Coordinated communication with internal and external stakeholders provides them with accurate and appropriate information needed to make risk-based decisions and ensure compliance with the IAC Cybersecurity Plan.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 8.3.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity monitoring program specifies internal and external stakeholders who will receive event detection information prior to an official declaration of an IAC Cyber Incident.
2) The IAC Cybersecurity monitoring program specifies what event detection information is communicated to both internal and external stakeholders.
3) The IAC Cybersecurity monitoring program requires that communication to external parties of event detection information is done so by authorized personnel only.

#### 8.3.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.3.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 8.3.4.4 Natural Gas Transmission Pipeline Supplemental Guidance

a) Special consideration should be given to the communication of event detection Information regarding FERC’s Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 8.3.5 DE.DP-5 – Continuous Improvement for Detection Processes

Continuous improvement calls for the refinement of detection processes through the monitoring and review of the IAC Cyber Environment to protect the security posture. Lessons learned are utilized for improvement and updates of the detection processes.

| | | |
|---|---|---|
| **P1:** (1); (2); | **P2:** (1); (2); | **P3:** (1); (2); |

#### 8.3.5.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that continuous improvement practices are employed for detection processes related to IAC Security Program and IAC Security Plan reviews required in Section 6.1 Governance (ID.GV) on page 25 above.
2) The IAC Cybersecurity Plan requires that continuous improvement practices for detection processes include reviewing lessons learned.

#### 8.3.5.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 8.3.5.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

# 9 ONG IAC Cybersecurity Profile Requirements - Respond (RS)

It is critical to the availability of IAC essential functions that organizations develop and implement a coordinated approach to incident response for their IAC Cyber Environments. The organization's mission, including its role in critical infrastructure, functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities.

An IAC incident response capability will enable a systematic approach to incidents, ensuring that the appropriate steps are taken. This structure will assist personnel in executing recovery more efficiently, thereby minimizing potential loss or disruption to IAC essential functions. Effective management of response plans can yield learnings that lead to stronger protections. This systematic approach and management of a response plan can improve response to future incidents.

## 9.1 Response Planning (RS.RP)

To effectively address an IAC cyber incident, an organization should have an incident response plan. The IAC cyber incident response plan should provide a roadmap for implementing the organization's cyber incident response capability. It should provide the high-level approach for how the incident response capability fits into the organization. The plan should be developed to meet the unique requirements of the organization's mission, size, structure, and functions, including its role in critical infrastructure. The resources and management support that is needed to effectively maintain and mature an IAC incident response capability should also be laid out in the plan.

### 9.1.1 RS.RP-1 – Cyber Incident Response Plan Execution

The organization's IAC cyber incident response plans should be exercised during or after a cyber event. To mitigate negative effects of response activities, the organization should respond to identified or detected cyber events according to procedures. Pre-defined procedures help to ensure that each team will take the appropriate sequence of actions depending on the type of incident.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 9.1.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan be activated upon the official declaration of an IAC Cyber Incident.

#### 9.1.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.1.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.1.1.4 Supplemental Guidance

a) Consideration should be given to leveraging and/or coordinating with existing incident, safety, and emergency response plans where appropriate.

## 9.2 Communications (RS.CO)

It is important that response activities are coordinated with internal and external stakeholders. This should also include external support from law enforcement agencies, as appropriate.

As part of a comprehensive incident response capability, organizations should consider the coordination and sharing of information with external service providers and IAC supply chain organizations.

### 9.2.1 RS.CO-1 – Cyber Incident Response Roles and Responsibilities

The organization should include the cyber-incident response team member's roles and responsibilities in any cyber-incident response plans, including all stakeholders. Response plans should ensure personnel understand objectives, restoration priorities, and assignment responsibilities for event or incident response—including an escalation process, that provides guidance on the different incident management and escalation roles and responsibilities. Prior to any incident response, relevant elements of the response plans should be communicated to those personnel responsible for or impacted by the planned response activities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); (5 | **P2:** (1); (2); (3); (4); (5); | **P3:** (1); (2); (3); (4); (5); |

#### 9.2.1.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan describes the structure and organization of the incident response capability including incident response roles, responsibilities, assigned individuals with contact information.
2) The IAC Cybersecurity Plan requires that copies of the IAC Cyber Incident Response Plan be distributed to incident response personnel and organizational stakeholders.
3) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan be updated to address changes to the organization or IAC Cyber Environment.
4) The IAC Cybersecurity Plan requires that changes to the IAC Cyber Incident Response Plan are communicated to incident response personnel and organizational stakeholders.
5) The IAC Cybersecurity Plan requires that periodic tests be conducted of the IAC Cyber Incident Response Plan to validate that roles, responsibilities, and order of operations are understood.

#### 9.2.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.2.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.2.1.4 Natural Gas Transmission Pipeline Supplemental Guidance

a) Special consideration should be given to cyber incident response role and responsibility assignments regarding FERC’s Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 9.2.2 RS.CO-2 – Incident Reporting

Organizations should have formal procedures which describe how and where employees, contractors, or others can report anomalous events, behaviors, or possible cybersecurity events. Mechanisms, such as forms and hotline call numbers, should be created to support the reporting action and to help the person reporting to remember all necessary actions in case of a cybersecurity event. The objective of incident reporting is to verify the cause of anomalous events, behaviors, and possible cybersecurity events and improve the response to determined cybersecurity incidents.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.2.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response capability provides a mechanism for personnel to report suspected security incidents, suspicious activity, and anomalous events.
2) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response capability communicate the mechanism for reporting suspected incidents.
3) The IAC Cyber Incident Response Plan defines the criteria for officially declaring the occurrence of an IAC cyber incident, which triggers the Cyber Incident Response Plan execution.

#### 9.2.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.2.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.2.2.4 Supplemental Guidance

a) Signs of vandalism or theft can be a cover for a cybersecurity event. All such events should be reviewed for potential cybersecurity relevant impact.

### 9.2.3 RS.CO-3 – Incident Information Sharing

After a cybersecurity incident has been formally declared, organizations should share incident information with stakeholders consistently, timely, and with established criteria per the cyber-incident response plan. Organizations should have defined mechanisms for escalation and reporting, and for notifying stakeholders. Without a pre-defined incident information sharing procedure, an incident may not be escalated or communicated to stakeholders, which may delay or compromise response activities.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.2.3.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan includes a communications plan which specifies internal and external stakeholders who will receive information during cyber incident response activities.
2) The IAC Cyber Incident Response Plan specifies what incident response information is communicated to both internal and external stakeholders.
3) The IAC Cyber Incident Response Plan requires that communication to external parties of incident response information is done so by authorized personnel only.

#### 9.2.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.2.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.2.3.4 Natural Gas Transmission Pipeline Supplemental Guidance

a) Special consideration should be given to incident information sharing regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 9.2.4 RS.CO-4 – Incident Response Stakeholder Coordination

Organizations and incident response teams should coordinate cybersecurity incident response actions with stakeholders—consistent with cyber-incident response plans. Response plans should contain mechanisms for how and when to collaborate with internal and external stakeholders, to effectively respond to and recover from the incident, and to solicit external support such as law enforcement agencies or cyber-incident response specialists. Stakeholders for cyber-incident response can include, mission/business owners, IAC Cyber Asset and system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, regulators, and procurement offices.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 9.2.4.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan includes processes for coordinating incident response activities with internal and external stakeholders.

#### 9.2.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.2.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.2.4.4 Supplemental Guidance

a) Where third parties or joint ventures are involved, organizations should develop guidelines for providing, requesting, and/or obtaining support from external partners to coordinate cyber-operations.

#### 9.2.4.5 Natural Gas Transmission Pipeline Supplemental Guidance

b) Special consideration should be given to incident response stakeholder coordination regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

### 9.2.5 RS.CO-5 – Information Sharing

Organizations and incident response teams should coordinate the sharing of cybersecurity event information with external stakeholders, such as industry security groups, regulators, or law enforcement agencies, to achieve broader cybersecurity awareness. Sharing should be based on risk assessment to decide whether cooperation and information sharing is warranted.

| | | |
|---|---|---|
| **P1:** None | **P2:** None | **P3:** None |

#### 9.2.5.1 Baseline Profile Requirements

No Baseline Profile specific requirements

#### 9.2.5.2 Enhanced Profile Requirements

No Enhanced Profile specific requirements.

#### 9.2.5.3 Extended Profile Requirements

No Extended Profile specific requirements.

#### 9.2.5.4 Supplemental Guidance

a) Organizations may consider participating in information sharing organizations which exist to assist with enhancing industry cybersecurity awareness.

b) Cybersecurity threats are sometimes targeted against an industry rather than a particular organization or asset, and participation in industry information training may help enhance cybersecurity preparedness.

c) Care should be given to ensure appropriate legal mechanisms are on in place (e.g. Non-disclosure Agreement) and the organization's legal department has been consulted prior to sharing non-public information with external parties.

## 9.3 Analysis (RS.AN)

Analysis is the first step in determining if an IAC cyber incident has or is occurring. Analysis also determines the scope and severity of potential impact to the IAC Cyber Environment and the IAC essential functions.

### 9.3.1 RS.AN-1 – Investigation of Notifications

Notifications alert organizations to possible cybersecurity incidents. Organizations and incident response teams should investigate notifications and determine an appropriate response. Timely investigations can expedite detection, response, and recovery efforts.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 9.3.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that notifications and alerts, whether from an automated system or human observation, are investigated.

#### 9.3.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.3.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.3.1.4 Supplemental Guidance

a) Non-invasive investigation techniques should be employed to prevent unintended consequences caused by IAC Essential Function distributions.

### 9.3.2 RS.AN-2 – Understanding Cyber Incident Impact

A Cyber incident impact assessment determines the potential scope and costs of a declared incident. This allows the organization to apply the appropriate level of resources to the incident.

Organizations and incident response teams should analyze and quantify the impact of a confirmed cyber incident on impacted IAC Cyber Assets in the zone in which it was detected, and other connected zones and conduits. Cyber incident impact assessments should be evaluated to improve an organization's cybersecurity program.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.3.2.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan includes processes to analyze an incident to understand the impact to IAC Cyber Assets within the IAC Segmented Environment in which it was detected.
2) The IAC Cyber Incident Response Plan includes processes to analyze an incident to understand the impact to other IAC Segmented Environments outside the IAC Segmented Environment in which it was detected.
3) The IAC Cyber Incident Response Plan includes processes to include incident impact analysis in lessons learned for the reduction in likelihood or impact of potential future incidents.

#### 9.3.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.3.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.3.2.4 Supplemental Guidance

a) The system nature of pipelines is such that the compromise of one IAC Cyber Asset or one IAC Segregated Environment may have an upstream or downstream impact, including the receipt or destination locations in ways that may not be readily apparent. The scope of the impact analysis should extend beyond the immediate IAC Security Zone or IAC Security Conduit to look for potential horizontal or lateral movement.
b) The use of Process Hazard Analysis (PHA) methods may be used to develop a greater understanding of potential negative impacts.
c) Other work being performed on the pipeline may affect the magnitude of the incident. Consideration should be given to account for these dynamic modifications.

### 9.3.3 RS.AN-3 – Forensic Analysis

Forensic analysis is a type of forensic science encompassing the recovery and investigation of material related to a cyber incident that is found in digital devices. It is a detailed investigation for detecting and documenting the course, perpetrators, and consequences of a security incident. Forensic analysis is often linked with evidence used in court proceedings for pursuing justice in criminal matters. It involves the use of a wide range of technologies and investigative methods and procedures.

Organizations and cyber-incident response teams should conduct forensic analysis on collected cybersecurity event information to determine root cause of an incident or failure and take action to prevent its reoccurrence. Organizations should have the capability to assist in or conduct forensic investigations of cybersecurity incidents and work with cyber-incident response teams to engineer protective and detective controls to facilitate the investigative process.

The objective of Forensic Analysis is the identification, collection, acquisition, and preservation of information, which can serve as evidence for the purposes of root cause analysis, pursuing criminal activities, and the reduction of risk of future cyber incidents.

| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |
|---|---|---|

#### 9.3.3.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan includes processes for the preservation of information, which can serve as evidence, including operations personnel training on appropriate actions to preserve potential evidence when anomalous events are suspected or detected.
2) The IAC Cyber Incident Response Plan includes processes for the identification, collection, and acquisition of information, which can serve as evidence.
3) The IAC Cyber Incident Response Plan includes processes for the forensic analysis of cyber incident evidence for the purpose of root cause analysis.
4) The IAC Cyber Incident Response Plan includes processes to include incident forensic analysis in lessons learned for the reduction in likelihood or impact of potential future incidents.

#### 9.3.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.3.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.3.3.4 Supplemental Guidance

a) If organizational personnel do not have sufficient skills or tools to conduct forensics of cyber incidents, then the organization should consider engaging external forensics resources for incidents requiring forensic investigation.
b) Pipeline IAC solutions are often critical to essential functions and putting them into an offline state to conduct forensics may not be readily available. Before an incident occurs, organizations should develop alternate methods of preserving and collecting forensic data from critical systems. These strategies may include IAC Essential Function redundancy, implementing automated security and operations event collection (e.g. log aggregation, SIEM), and the like.
c) The firmware in some IAC Cyber Assets are not supported by IT or PC centric forensics tools. In this cased forensic analysis may need to be performed by digital forensic specialists.
d) Limitations in IAC Cyber Asset network connectivity or network bandwidth my hinder some forensic data collection techniques. In these cases, alternate means of forensic data collection should be pursued (e.g. local log collection to offline collector)

### 9.3.4 RS.AN-4 – Cyber Incident Categorization

Cyber incident categorization is the process of classifying a cyber incident by causation, potential and real impacts, nature (exploitive or disruptive) and other attributes to help apply the appropriate resources to address the scope, severity, and impact of the incident.

The highest risk exposure of IAC Cyber Environments is often assessed to be from the loss of availability or the loss of process data integrity. Cyber Incident Categorization is especially important for incidents involving IAC Cyber Environments to understand the capability of the threat for any current or future potential disruption to availability or process data integrity.

The objective of Cyber Incident categorization is to help engage the resources needed to address a cyber incident as effectively as possible.

| **P1:** (1); (2); (3); (4); (5); (6); (7); ( | **P2:** (1); (2); (3); (4); (5); (6); (7); | **P3:** (1); (2); (3); (4); (5); (6); (7); |
|---|---|---|

#### 9.3.4.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan categorize IAC Cyber incidents as part of the declaration process to drive the appropriate incident response.
2) The IAC Cybersecurity Plan requires that consistent criteria be used to define IAC cyber incident categorization attributes.
3) The IAC Cybersecurity Plan requires that the API 1164 Business Objective Impact Classification Matrix be considered when defining IAC cyber incident categorization attributes.

4) The IAC Cybersecurity Plan requires that an Incident be classified by its ability to disrupt IAC essential functions.
5) The IAC Cybersecurity Plan requires that an Incident Type (e.g. DDOS, Malware, Unauthorized access), is used in the categorization of an IAC cyber incident.
6) The IAC Cybersecurity Plan requires that an Incident severity ranking (e.g. High, med, low; 1, 2, 3…) is used in the categorization of an IAC cyber incident.
7) The IAC Cybersecurity Plan requires that an incident sensitivity level be used in the categorization of an IAC cyber incident (e.g. Highly Sensitive: potential inappropriate personnel activity).

#### 9.3.4.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.3.4.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.3.4.4 Supplemental Guidance

a) Organizations and cyber-incident response teams should categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.
b) Organizations and cyber-incident response teams should identify classes of incidents and define actions to take in response to classes of incidents that help safeguard against IAC Essential Function disruptions.
c) Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks.
d) Appropriate incident response actions may include, for example, graceful degradation, system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or placing systems in an operating mode that is reserved solely for when systems are under attack.
e) Post incident reviews should be conducted to confirm an incident or event was classified appropriately.

### 9.3.5 RS.AN-5 – Analysis of Vulnerabilities from Internal and External Sources

Requirements for this section are covered under Section 7.4.12 PR.IP-12 –Vulnerability Management Plan on page 73 above.

| | | |
|---|---|---|
| **P1:** None | **P2:** None | **P3:** None |

#### 9.3.5.1 Baseline Profile Requirements

No Baseline Profile specific requirements.

#### 9.3.5.2 Enhanced Profile Requirements

No Enhanced Profile specific requirements.

#### 9.3.5.3 Extended Profile Requirements

No Extended Profile specific requirements.

#### 9.3.5.4 Supplemental Guidance

a) Consider adding vulnerability disclosure requirements IAC Cyber Asset or IAC Cyber System purchasing requirements.

## 9.4 Mitigation (RS.MI)

Cyber Security mitigation is the act of identifying, documenting, and taking steps to reduce vulnerabilities with the intent to prevent or contain the expansion of an incident. Mitigation of vulnerabilities helps organizations to minimize cyber security incidents and data breaches as well as limit the damage caused by an incident. Mitigation strategies help counter a range of exploitation techniques used by cyber attackers.

### 9.4.1 RS.MI-1 – Incident Containment

Incident Containment limits further damage and preserves forensic evidence of the attack. Proper containment of an incident will allow organizations to investigate and identify critical elements used in the attack to build stronger cyber protections to minimize future attacks.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.4.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan include incident containment processes.
2) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan include incident response escalation processes to promptly engage the management level sufficient to authorize the necessary steps to contain an IAC Cyber Incident.
3) The IAC Cyber Incident Response Plan includes processes to include containment actions in lessons learned for the reduction in likelihood or impact of potential future incidents.

#### 9.4.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.4.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.4.1.4 Supplemental Guidance

a) Pipeline sites are often unmanned, and special consideration should be given for cases where a physical presence may be required to contain the impact of a cyber incident.

a) Consider the API 1164 impact rating of the IAC Segregated Environment when implementing containment controls.

b) Consider unintended consequences and impacts to essential services if implementing containment techniques such as network shutdown, IAC Cyber Asset or IAC Segregated Environment isolation, or full pipeline shutdown. or isolation mode in the event of a cyber incident. Consider manual mode of operations where feasible, or pipeline shutdown.

### 9.4.2 RS.MI-2 – Incident Mitigation

Incident mitigation includes planning the response to an incident, allowing an organization to follow processes that will assist in reducing the impact. Organizations are more likely to limit damage when they detect and respond to an incident by executing planned actions. Minimizing cyber incident impact both current and future is the primary objective of incident mitigation.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.4.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include incident mitigation processes.
2) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan include incident response escalation processes to promptly engage the management level sufficient to authorize the necessary steps to mitigate an IAC Cyber Incident.
3) The IAC Cyber Incident Response Plan includes processes to include mitigation actions in lessons learned for the reduction in likelihood or impact of potential future incident.

#### 9.4.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.4.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.4.2.4 Supplemental Guidance

a) Pipeline sites are often unmanned, and special consideration should be given for cases where a physical presence may be required to mitigate the impact of a cyber incident.

b) To address geographically distributed nature and often the remoteness of pipeline IAC Cyber Assets consider the following as possible cyber incident mitigation techniques: redundancy, real-time monitoring for fast incident detection, maintaining spare equipment, gold images, and regional/distributed personnel.

c) Consider establishing acceptable meantime to restoration criteria based on the API 1164 Impact Assessment.

### 9.4.3 RS.MI-3 – Newly Identified Vulnerabilities

Organizations should take steps to document newly identified vulnerabilities during an incident. Documenting the vulnerabilities of an IAC Cyber Environment and how the vulnerabilities can be exploited help identify the risk exposure to that environment. Understanding the vulnerabilities and the organizations response to mitigate or accept risk will assist in detecting or preventing future cyber-attacks.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); | **P2:** (1); (2); (3); | **P3:** (1); (2); (3); |

#### 9.4.3.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan include processes to address new vulnerabilities identified during the incident response activities.

2) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan processes document or mitigate newly identified vulnerabilities.

3) The IAC Cybersecurity Plan requires that The IAC Cyber Incident Response Plan integrate with the processes specified in the Vulnerability Management Plan to address newly identified vulnerabilities.

See Section 7.4.12 PR.IP-12 –Vulnerability Management Plan on page 73, above.

#### 9.4.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.4.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

## 9.5 Improvements (RS.IM)

Organizational response activities should be improved by incorporating lessons learned from current and previous detection/response activities.

### 9.5.1 RS.IM-1 – Response Plans Lessons Learned

Lessons learned session should be held by all incident Response Team members to discuss what was learned from the incident. Determine what worked well in your response plan, and where there were some holes. Updating your response plans with lessons learned from both mock and real incidents will help strengthen your systems against the future attacks as well as improve the team's future incident response performance.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 9.5.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes to identify response lessons learned during and after each execution of the Plan whether for an actual incident or for plan testing.

2) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes to review response lessons learned after each execution of the Plan.

3) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan's continuous improvement processes review the response lessons learned process.

4) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan's continuous improvement processes generate, and track response lessons learned action items to completion.

#### 9.5.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.5.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 9.5.2 RS.IM-2 – Response Strategy Updates

Up-to-date and practiced response strategies can significantly reduce the impact of an incident. Response strategies should be updated from lessons learned, new technologies, changes in the computing environment, as well as new vulnerabilities and threats facing the organization.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 9.5.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes that review lessons learned for potential response strategy updates.

#### 9.5.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 9.5.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 9.5.2.4 Supplemental Guidance

a) Consider updates to the strategy to address changes to the organization, IAC Cyber Environment, and problems encountered during plan implementation, execution, or testing.

## 10 ONG IAC Cybersecurity Profile Requirements - Recover (RC)

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. The target profile outcome categories and subcategories within this function are detailed below.

### 10.1 Recovery Planning (RC.RP):

Recovery processes and procedures are maintained and executed to ensure timely restoration of IAC essential functions affected by cybersecurity incidents.

#### 10.1.1 RC.RP-1 – Incident Recovery

Incident recovery is the process where any IAC essential functions impacted by a cyber incident are restored to normal operations. Recovery may involve activities such as restoring IAC Cyber Assets from clean backups, rebuilding IAC Cyber Assets, replacing compromised files, or installing patches. Impacted IAC Segregated Environments and their IAC Cyber Assets may be hardened to prevent similar incidents.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 10.1.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan initiate the recovery processes as soon as practicable.

#### 10.1.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 10.1.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 10.1.1.4 Supplemental Guidance

a) When multiple IAC Segregated Environments or IAC Cyber Assets are impacted, restoration prioritization should be given to those causing the highest impact from loss or disruption of IAC essential functions.

b) The organization may consider employing higher levels of system logging or network monitoring as part of the IAC Cyber Environment recovery process.

c) Cyber response teams may consider having “away-kits” prepared to quickly relocate to remote locations. The plan and kit should function in case network connectivity is unavailable at a remote site.

## 10.2 Improvements (RC.IM)

IAC Cyber incident recovery planning and processes are improved by incorporating lessons learned into future activities. Processes should be kept current, including any necessary corrections and addition of new information.

### 10.2.1 RC.IM-1 – Recovery Lessons Learned

Updates to the IAC Cyber recovery plans and processes should seek out lessons learned and incorporate them into the plan updates. This is important because lessons learned may uncover information that was unforeseen and not included in the original plan. The objective is to consider all lessons learned whenever a recovery process is executed or tested to enhance incident response recovery execution.

| | | |
|---|---|---|
| **P1:** (1); (2); (3); (4); | **P2:** (1); (2); (3); (4); | **P3:** (1); (2); (3); (4); |

#### 10.2.1.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes to identify recovery lessons learned during and after each execution of the Plan whether for an actual incident or for plan testing.

2) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes to review recovery lessons learned after each execution of the Plan.

3) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan’s continuous improvement processes review the recovery lessons learned process.

4) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan’s continuous improvement processes generate, and track recovery lessons learned action items to completion.

#### 10.2.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 10.2.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 10.2.1.4 Supplemental Guidance

a) Consider incorporating lessons learned from not only previous incidents but also publicly available intelligence. Government, media outlets, and industry are public information sources.

b) Organizations should consider drawing on lessons learned from IT cyber incidents, where they are like the IAC Cyber Environments.

### 10.2.2 RC.IM-2 – Recovery Strategy Updates

The IAC Cyber Recovery strategies should be updated whenever a recovery process is executed or tested. This is important to IAC cybersecurity because deficiencies found during each execution of the process need to be corrected in the plan to maintain current and effective recovery strategies. The objective is to ensure that the IAC Cyber Recovery strategies are as current and robust as possible.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 10.2.2.1 Baseline Profile Requirements

1) The IAC Cybersecurity Plan requires that the IAC Cyber Incident Response Plan include continuous improvement processes that review lessons learned for potential recovery strategy updates.

#### 10.2.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 10.2.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

## 10.3 Communications (RC.CO)

The restoration of IAC essential functions and services includes communication and coordination with internal and external stakeholders, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. This coordination is important to help other teams synchronize their own processes and communications (e.g. the standing-down of first responder readiness teams).

### 10.3.1 RC.CO-1 – Managing Public Relations

The restoration of IAC essential functions and services includes communication and coordination with internal stakeholders who are responsible for managing public relations regarding IAC Cyber Incident activities. The objective of Managing Public Relations within the Incident Recovery process is to relay accurate information to external stakeholders and address potential misinformation.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 10.3.1.1 Baseline Profile Requirements

1) IAC Cyber Incident Response Plan specifies internal stakeholders who are responsible for managing public relations regarding IAC Cyber Incident activities.

#### 10.3.1.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 10.3.1.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

#### 10.3.1.4 Supplemental Guidance

a) The organization should consider training or other methods of education to ensure all personnel involved in a cyber incident response are not allowed to communicate about a cyber incident unless they are explicitly authorized to do so.

### 10.3.2 RC.CO-2 – Reputation Repair

Any reportable IAC cyber incident can influence the reputation of the company and business unit where it occurs. The repair of this reputation could be significant and therefore needs to be handled in a professional and timely manner by company assigned or appointed representatives.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

#### 10.3.2.1 Baseline Profile Requirements

1) IAC Cyber Incident Response Plan identifies internal stakeholders who are responsible for repairing reputation damage resulting from an IAC Cyber Incident.

#### 10.3.2.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

#### 10.3.2.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 10.3.3 RC.CO-3 – Communicating Recovery Activities

Following an IAC cyber incident, recovery operations and activities should be communicated to all stakeholders keeping them current on efforts to return the affected systems to a proper operating condition.

| | | |
|---|---|---|
| **P1:** (1); | **P2:** (1); | **P3:** (1); |

### 10.3.3.1 Baseline Profile Requirements

1) The IAC Cyber Incident Response Plan includes a communications plan which specifies internal and external stakeholders who will receive information regarding cyber incident recovery activities.

### 10.3.3.2 Enhanced Profile Requirements

See P2 in table above for Enhanced Profile requirements.

### 10.3.3.3 Extended Profile Requirements

See P3 in table above for Extended Profile requirements.

### 10.3.3.4 Natural Gas Transmission Pipeline Supplemental Guidance

a) Special consideration should be given to recovery activity communications regarding FERC's Standards of Conduct (SOC) requirements for Transmission Function Employees and Marketing Function Employees compliance with the disclosure of Non-public Transmission Function Information.

## Bibliography

All of the related authority and references cited in this document should be viewed as living documents. They are subject to change, modification, update, and rescission. As of the writing of this document, this is the current list.

1. Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, February 12, 2013.
2. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, https://www.federalregister.gov/d/2013-03915
3. U.S. Transportation Security Administration, *Pipeline Security Guidelines*, Mar. 2018
4. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*, Apr. 16, 2018
5. International Society of Automation (ISA) / International Electrotechnical Commission (IEC), *62443-2-1 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*, Nov. 2010.
6. International Society of Automation (ISA) / International Electrotechnical Commission (IEC), *62443-2-4 Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*, Jun. 2015.
7. International Society of Automation (ISA) / International Electrotechnical Commission (IEC), *62443-3-3 Security for industrial automation and control systems– Part 3-3: System security requirements and security levels*, Aug. 2013.
8. International Society of Automation (ISA) / International Electrotechnical Commission (IEC), *62443-4-1 Industrial communication networks – Network and system security – Part 4-1: Secure product development lifecycle requirements*, Jan. 2018.
9. National Institute of Standards and Technology (NIST), Special Publication 800-53 - *Security and Privacy Controls for Federal Information Systems and Organizations, revision 4*, Apr. 2013.
10. National Institute of Standards and Technology (NIST), Special Publication 800-88 – Guidelines for Media Sanitization*, revision 1*, Dec. 2014.
11. Interstate Natural Gas Association of America (INGAA), “Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry”. http://ics-cert.us-cert.gov/Standards-and-References
12. U.S. Government Accountability Office, GAO-19-14
13. The DHS Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors
14. U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, “Computer Security Incident Handling Guide.” http://csrc.nist.gov/publications/PubsSPs.html

# ANNEX A

## Business Objectives to API 1164 Control Subcategories

(informative)

In the Function tables below, for each business objective, the most critical Subcategories initially determined to support the objective are highlighted with the associate Function color. Items highlighted in gold have been identified as TSA specified cybersecurity requirements.

**Table** Error! No text of specified style in document.**-1: Identify Mapped Business Objectives**

| IDENTIFY | **Maintain Human Safety** | **Maintain Environment Safety** | **Maintain Property Safety** | **Maintain Operations Capability** | **Maintain Reputation** | **Maintain Compliance Posture** |
|---|---|---|---|---|---|---|
| Governance | ID.GV-1 | ID.GV-1 | ID.GV-1 | ID.GV-1 | ID.GV-1 | ID.GV-1 |
| | ID.GV-2 | ID.GV-2 | ID.GV-2 | ID.GV-2 | ID.GV-2 | ID.GV-2 |
| | ID.GV-3 | ID.GV-3 | ID.GV-3 | ID.GV-3 | ID.GV-3 | ID.GV-3 |
| | ID.GV-4 | ID.GV-4 | ID.GV-4 | ID.GV-4 | ID.GV-4 | ID.GV-4 |
| Risk Management Strategy | ID.RM-1 | ID.RM-1 | ID.RM-1 | ID.RM-1 | ID.RM-1 | ID.RM-1 |
| | ID.RM-2 | ID.RM-2 | ID.RM-2 | ID.RM-2 | ID.RM-2 | ID.RM-2 |
| | ID.RM-3 | ID.RM-3 | ID.RM-3 | ID.RM-3 | ID.RM-3 | ID.RM-3 |
| Business Environment | ID.BE-1 | ID.BE-1 | ID.BE-1 | ID.BE-1 | ID.BE-1 | ID.BE-1 |
| | ID.BE-2 | ID.BE-2 | ID.BE-2 | ID.BE-2 | ID.BE-2 | ID.BE-2 |
| | ID.BE-3 | ID.BE-3 | ID.BE-3 | ID.BE-3 | ID.BE-3 | ID.BE-3 |
| | ID.BE-4 | ID.BE-4 | ID.BE-4 | ID.BE-4 | ID.BE-4 | ID.BE-4 |
| | ID.BE-5 | ID.BE-5 | ID.BE-5 | ID.BE-5 | ID.BE-5 | ID.BE-5 |
| Supply Chain Risk Management | ID.SC-1 | ID.SC-1 | ID.SC-1 | ID.SC-1 | ID.SC-1 | ID.SC-1 |
| | ID.SC-2 | ID.SC-2 | ID.SC-2 | ID.SC-2 | ID.SC-2 | ID.SC-2 |
| | ID.SC-3 | ID.SC-3 | ID.SC-3 | ID.SC-3 | ID.SC-3 | ID.SC-3 |
| | ID.SC-4 | ID.SC-4 | ID.SC-4 | ID.SC-4 | ID.SC-4 | ID.SC-4 |
| | ID.SC-5 | ID.SC-5 | ID.SC-5 | ID.SC-5 | ID.SC-5 | ID.SC-5 |
| Risk Assessment | ID.RA-1 | ID.RA-1 | ID.RA-1 | ID.RA-1 | ID.RA-1 | ID.RA-1 |
| | ID.RA-2 | ID.RA-2 | ID.RA-2 | ID.RA-2 | ID.RA-2 | ID.RA-2 |
| | ID.RA-3 | ID.RA-3 | ID.RA-3 | ID.RA-3 | ID.RA-3 | ID.RA-3 |
| | ID.RA-4 | ID.RA-4 | ID.RA-4 | ID.RA-4 | ID.RA-4 | ID.RA-4 |
| | ID.RA-5 | ID.RA-5 | ID.RA-5 | ID.RA-5 | ID.RA-5 | ID.RA-5 |
| | ID.RA-6 | ID.RA-6 | ID.RA-6 | ID.RA-6 | ID.RA-6 | ID.RA-6 |
| Asset Management | ID.AM-1 | ID.AM-1 | ID.AM-1 | ID.AM-1 | ID.AM-1 | ID.AM-1 |
| | ID.AM-2 | ID.AM-2 | ID.AM-2 | ID.AM-2 | ID.AM-2 | ID.AM-2 |
| | ID.AM-3 | ID.AM-3 | ID.AM-3 | ID.AM-3 | ID.AM-3 | ID.AM-3 |
| | ID.AM-4 | ID.AM-4 | ID.AM-4 | ID.AM-4 | ID.AM-4 | ID.AM-4 |
| | ID.AM-5 | ID.AM-5 | ID.AM-5 | ID.AM-5 | ID.AM-5 | ID.AM-5 |
| | ID.AM-6 | ID.AM-6 | ID.AM-6 | ID.AM-6 | ID.AM-6 | ID.AM-6 |

**Table** Error! No text of specified style in document.**-2: Protect Mapped Business Objectives**

| PROTECT | **Maintain Human Safety** | **Maintain Environment Safety** | **Maintain Property Safety** | **Maintain Operational Capability** | **Maintain Reputation** | **Maintain Compliance Posture** |
|---|---|---|---|---|---|---|
| Access Control | PR.AC-1 | PR.AC-1 | PR.AC-1 | PR.AC-1 | PR.AC-1 | PR.AC-1 |
| | PR.AC-2 | PR.AC-2 | PR.AC-2 | PR.AC-2 | PR.AC-2 | PR.AC-2 |
| | PR.AC-3 | PR.AC-3 | PR.AC-3 | PR.AC-3 | PR.AC-3 | PR.AC-3 |
| | PR.AC-4 | PR.AC-4 | PR.AC-4 | PR.AC-4 | PR.AC-4 | PR.AC-4 |
| | PR.AC-5 | PR.AC-5 | PR.AC-5 | PR.AC-5 | PR.AC-5 | PR.AC-5 |
| | PR.AC-6 | PR.AC-6 | PR.AC-6 | PR.AC-6 | PR.AC-6 | PR.AC-6 |
| | PR.AC-7 | PR.AC-7 | PR.AC-7 | PR.AC-7 | PR.AC-7 | PR.AC-7 |
| Awareness and Training | PR.AT-1 | PR.AT-1 | PR.AT-1 | PR.AT-1 | PR.AT-1 | PR.AT-1 |
| | PR.AT-2 | PR.AT-2 | PR.AT-2 | PR.AT-2 | PR.AT-2 | PR.AT-2 |
| | PR.AT-3 | PR.AT-3 | PR.AT-3 | PR.AT-3 | PR.AT-3 | PR.AT-3 |
| | PR.AT-4 | PR.AT-4 | PR.AT-4 | PR.AT-4 | PR.AT-4 | PR.AT-4 |
| | PR.AT-5 | PR.AT-5 | PR.AT-5 | PR.AT-5 | PR.AT-5 | PR.AT-5 |
| Data Security | PR.DS-1 | PR.DS-1 | PR.DS-1 | PR.DS-1 | PR.DS-1 | PR.DS-1 |
| | PR.DS-2 | PR.DS-2 | PR.DS-2 | PR.DS-2 | PR.DS-2 | PR.DS-2 |
| | PR.DS-3 | PR.DS-3 | PR.DS-3 | PR.DS-3 | PR.DS-3 | PR.DS-3 |
| | PR.DS-4 | PR.DS-4 | PR.DS-4 | PR.DS-4 | PR.DS-4 | PR.DS-4 |
| | PR.DS-5 | PR.DS-5 | PR.DS-5 | PR.DS-5 | PR.DS-5 | PR.DS-5 |
| | PR.DS-6 | PR.DS-6 | PR.DS-6 | PR.DS-6 | PR.DS-6 | PR.DS-6 |
| | PR.DS-7 | PR.DS-7 | PR.DS-7 | PR.DS-7 | PR.DS-7 | PR.DS-7 |
| | PR.DS-8 | PR.DS-8 | PR.DS-8 | PR.DS-8 | PR.DS-8 | PR.DS-8 |
| Info Protection Processes | PR.IP-1 | PR.IP-1 | PR.IP-1 | PR.IP-1 | PR.IP-1 | PR.IP-1 |
| | PR.IP-2 | PR.IP-2 | PR.IP-2 | PR.IP-2 | PR.IP-2 | PR.IP-2 |
| | PR.IP-3 | PR.IP-3 | PR.IP-3 | PR.IP-3 | PR.IP-3 | PR.IP-3 |
| | PR.IP-4 | PR.IP-4 | PR.IP-4 | PR.IP-4 | PR.IP-4 | PR.IP-4 |
| | PR.IP-5 | PR.IP-5 | PR.IP-5 | PR.IP-5 | PR.IP-5 | PR.IP-5 |
| | PR.IP-6 | PR.IP-6 | PR.IP-6 | PR.IP-6 | PR.IP-6 | PR.IP-6 |
| | PR.IP-7 | PR.IP-7 | PR.IP-7 | PR.IP-7 | PR.IP-7 | PR.IP-7 |
| | PR.IP-8 | PR.IP-8 | PR.IP-8 | PR.IP-8 | PR.IP-8 | PR.IP-8 |
| | PR.IP-9 | PR.IP-9 | PR.IP-9 | PR.IP-9 | PR.IP-9 | PR.IP-9 |
| | PR.IP-10 | PR.IP-10 | PR.IP-10 | PR.IP-10 | PR.IP-10 | PR.IP-10 |
| | PR.IP-11 | PR.IP-11 | PR.IP-11 | PR.IP-11 | PR.IP-11 | PR.IP-11 |
| | PR.IP-12 | PR.IP-12 | PR.IP-12 | PR.IP-12 | PR.IP-12 | PR.IP-12 |
| Maintenance | PR.MA-1 | PR.MA-1 | PR.MA-1 | PR.MA-1 | PR.MA-1 | PR.MA-1 |
| | PR.MA-2 | PR.MA-2 | PR.MA-2 | PR.MA-2 | PR.MA-2 | PR.MA-2 |
| Protective Technology | PR.PT-1 | PR.PT-1 | PR.PT-1 | PR.PT-1 | PR.PT-1 | PR.PT-1 |
| | PR.PT-2 | PR.PT-2 | PR.PT-2 | PR.PT-2 | PR.PT-2 | PR.PT-2 |
| | PR.PT-3 | PR.PT-3 | PR.PT-3 | PR.PT-3 | PR.PT-3 | PR.PT-3 |
| | PR.PT-4 | PR.PT-4 | PR.PT-4 | PR.PT-4 | PR.PT-4 | PR.PT-4 |
| | PR.PT-5 | PR.PT-5 | PR.PT-5 | PR.PT-5 | PR.PT-5 | PR.PT-5 |

**Table** Error! No text of specified style in document.**-3: Detect Mapped Business Objectives**

| DETECT | **Maintain Human Safety** | **Maintain Environmental Safety** | **Maintain Property Safety** | **Maintain Operational Capability** | **Maintain Reputation** | **Maintain Compliance Posture** |
|---|---|---|---|---|---|---|
| Access Control | DE.AE-1 | DE.AE-1 | DE.AE-1 | DE.AE-1 | DE.AE-1 | DE.AE-1 |
| | DE.AE-2 | DE.AE-2 | DE.AE-2 | DE.AE-2 | DE.AE-2 | DE.AE-2 |
| | DE.AE-3 | DE.AE-3 | DE.AE-3 | DE.AE-3 | DE.AE-3 | DE.AE-3 |
| | DE.AE-4 | DE.AE-4 | DE.AE-4 | DE.AE-4 | DE.AE-4 | DE.AE-4 |
| | DE.AE-5 | DE.AE-5 | DE.AE-5 | DE.AE-5 | DE.AE-5 | DE.AE-5 |
| Data Security | DE.CM-1 | DE.CM-1 | DE.CM-1 | DE.CM-1 | DE.CM-1 | DE.CM-1 |
| | DE.CM-2 | DE.CM-2 | DE.CM-2 | DE.CM-2 | DE.CM-2 | DE.CM-2 |
| | DE.CM-3 | DE.CM-3 | DE.CM-3 | DE.CM-3 | DE.CM-3 | DE.CM-3 |
| | DE.CM-4 | DE.CM-4 | DE.CM-4 | DE.CM-4 | DE.CM-4 | DE.CM-4 |
| | DE.CM-5 | DE.CM-5 | DE.CM-5 | DE.CM-5 | DE.CM-5 | DE.CM-5 |
| | DE.CM-6 | DE.CM-6 | DE.CM-6 | DE.CM-6 | DE.CM-6 | DE.CM-6 |
| | DE.CM-7 | DE.CM-7 | DE.CM-7 | DE.CM-7 | DE.CM-7 | DE.CM-7 |
| | DE.CM-8 | DE.CM-8 | DE.CM-8 | DE.CM-8 | DE.CM-8 | DE.CM-8 |
| Protective Technology | DE.DP-1 | DE.DP-1 | DE.DP-1 | DE.DP-1 | DE.DP-1 | DE.DP-1 |
| | DE.DP-2 | DE.DP-2 | DE.DP-2 | DE.DP-2 | DE.DP-2 | DE.DP-2 |
| | DE.DP-3 | DE.DP-3 | DE.DP-3 | DE.DP-3 | DE.DP-3 | DE.DP-3 |
| | DE.DP-4 | DE.DP-4 | DE.DP-4 | DE.DP-4 | DE.DP-4 | DE.DP-4 |
| | DE.DP-5 | DE.DP-5 | DE.DP-5 | DE.DP-5 | DE.DP-5 | DE.DP-5 |

**Table** Error! No text of specified style in document.**-4: Respond Mapped Business Objectives**

| RESPOND | **Maintain Human Safety** | **Maintain Environmental Safety** | **Maintain Property Safety** | **Maintain Operational Capability** | **Maintain Reputation** | **Maintain Compliance Posture** |
|---|---|---|---|---|---|---|
| Response Planning | RS.RP-1 | RS.RP-1 | RS.RP-1 | RS.RP-1 | RS.RP-1 | RS.RP-1 |
| Communications | RS.CO-1 | RS.CO-1 | RS.CO-1 | RS.CO-1 | RS.CO-1 | RS.CO-1 |
| | RS.CO-2 | RS.CO-2 | RS.CO-2 | RS.CO-2 | RS.CO-2 | RS.CO-2 |
| | RS.CO-3 | RS.CO-3 | RS.CO-3 | RS.CO-3 | RS.CO-3 | RS.CO-3 |
| | RS.CO-4 | RS.CO-4 | RS.CO-4 | RS.CO-4 | RS.CO-4 | RS.CO-4 |
| | RS.CO-5 | RS.CO-5 | RS.CO-5 | RS.CO-5 | RS.CO-5 | RS.CO-5 |
| Analysis | RS.AN-1 | RS.AN-1 | RS.AN-1 | RS.AN-1 | RS.AN-1 | RS.AN-1 |
| | RS.AN-2 | RS.AN-2 | RS.AN-2 | RS.AN-2 | RS.AN-2 | RS.AN-2 |
| | RS.AN-3 | RS.AN-3 | RS.AN-3 | RS.AN-3 | RS.AN-3 | RS.AN-3 |
| | RS.AN-4 | RS.AN-4 | RS.AN-4 | RS.AN-4 | RS.AN-4 | RS.AN-4 |
| | RS.AN-5 | RS.AN-5 | RS.AN-5 | RS.AN-5 | RS.AN-5 | RS.AN-5 |
| Mitigation | RS.MI-1 | RS.MI-1 | RS.MI-1 | RS.MI-1 | RS.MI-1 | RS.MI-1 |
| | RS.MI-2 | RS.MI-2 | RS.MI-2 | RS.MI-2 | RS.MI-2 | RS.MI-2 |
| | RS.MI-3 | RS.MI-3 | RS.MI-3 | RS.MI-3 | RS.MI-3 | RS.MI-3 |
| Improvements | RS.IM-1 | RS.IM-1 | RS.IM-1 | RS.IM-1 | RS.IM-1 | RS.IM-1 |
| | RS.IM-2 | RS.IM-2 | RS.IM-2 | RS.IM-2 | RS.IM-2 | RS.IM-2 |

**Table** Error! No text of specified style in document.**-5: Recover Mapped Business Objectives**

| RECOVER | **Maintain Human Safety** | **Maintain Environmental Safety** | **Maintain Property Safety** | **Maintain Operational Capability** | **Maintain Reputation** | **Maintain Compliance Posture** |
|---|---|---|---|---|---|---|
| Recovery Planning | RC.RP-1 | RC.RP-1 | RC.RP-1 | RC.RP-1 | RC.RP-1 | RC.RP-1 |
| Improvements | RC.IM-1 | RC.IM-1 | RC.IM-1 | RC.IM-1 | RC.IM-1 | RC.IM-1 |
| | RC.IM-2 | RC.IM-2 | RC.IM-2 | RC.IM-2 | RC.IM-2 | RC.IM-2 |
| Communications | RC.CO-1 | RC.CO-1 | RC.CO-1 | RC.CO-1 | RC.CO-1 | RC.CO-1 |
| | RC.CO-2 | RC.CO-2 | RC.CO-2 | RC.CO-2 | RC.CO-2 | RC.CO-2 |
| | RC.CO-3 | RC.CO-3 | RC.CO-3 | RC.CO-3 | RC.CO-3 | RC.CO-3 |

This Page is Intentionally Left Blank