API Standard 1164, 3rd Edition:

The Biggest Impact to IAC Cybersecurity in a Decade

Cybersecurity for the Natural Gas and Oil Industry

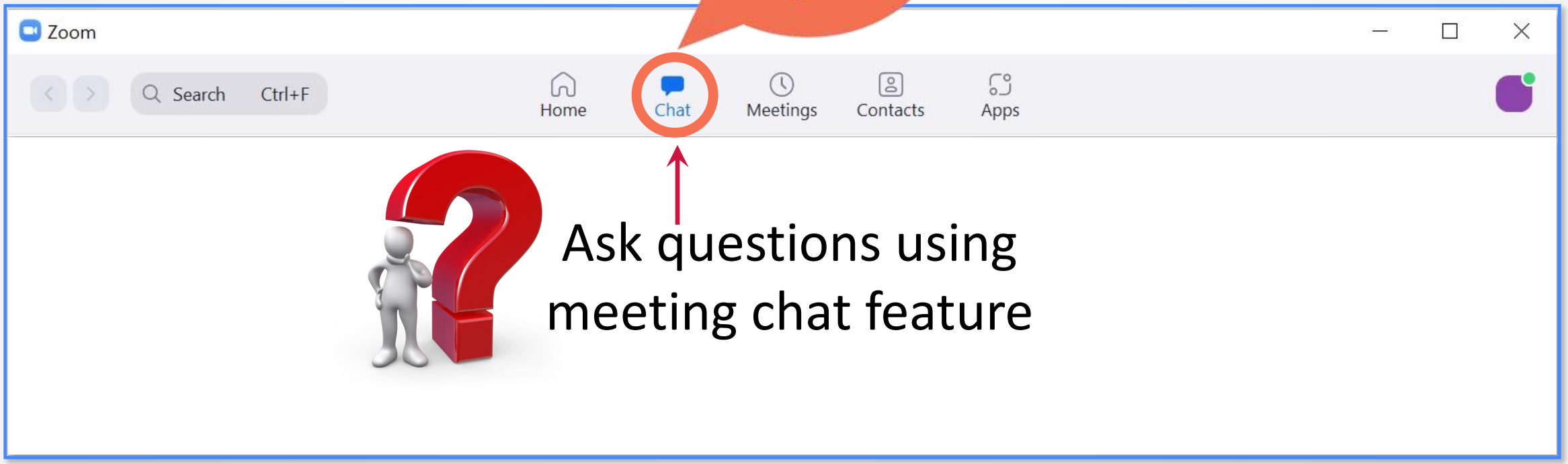
Hosted by the U.S. Energy Association (USEA)
through the
U.S. Agency for International Development's U.S. – Asia Gas Partnership

API

USEA
United States Energy Association

USAID
FROM THE AMERICAN PEOPLE

September 2021



Ask questions using meeting chat feature

USEA United States Energy Association

API

Today's Topics

- Rationale for Changes in the 3rd Edition
- Overview of the new 1164
- Review of Major Advances
- Question & Answer

United States Energy Association

Today's Speakers

- James Simmons, Shell Pipeline
- Tom Aubuchon, Ethosecure Consulting

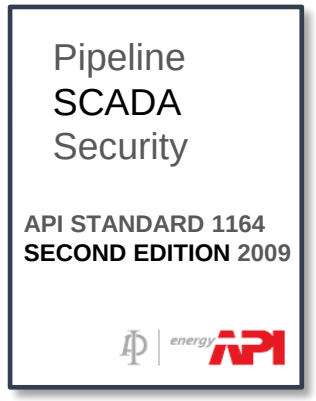
United States Energy Association

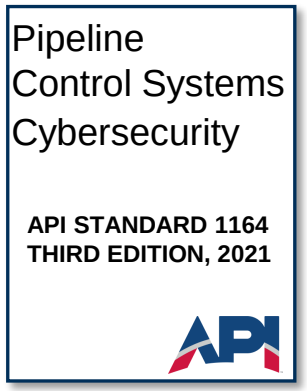
James Simmons

Infrastructure and Automation Manager, Shell Pipeline Co LP

Chair - API 1164 3rd Edition Working Group

- 20 years Pipeline Operations,
- 15 years SCADA Management
- 15 years OT Security
- Former Chair, API Cybernetics Committee
- Operations Security Officer, Shell Pipeline
- 8 years, U.S. Naval Nuclear Engineer
- Based in Houston, TX





Tom Aubuchon, CISM

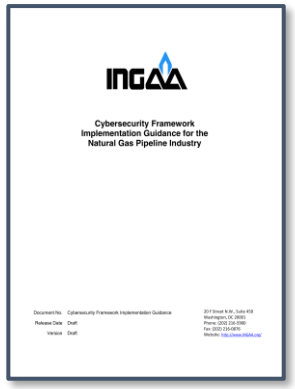
Principal Consultant, ETHOSECURE Consulting

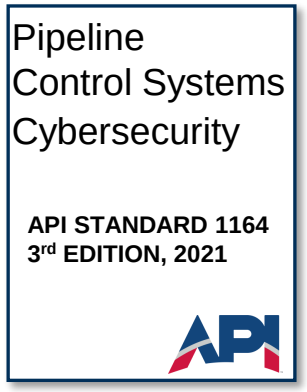
Co-Chair, Principal Author - API 1164 3rd Ed. Working Group (May 2018 – Jan 2021)

Consultant - API 1164 (Jan 2018 – Present)

Email: tom.aubuchon@ethosecure.com

- 38+ years of experience in OT, IT, and Product development, architecture, design and security.
- 26+ years experience in OT Security
- 24+ year ONG Pipeline industry
- 15+ years experience in IT Security
- Based in Houston, TX





Rationale for Change

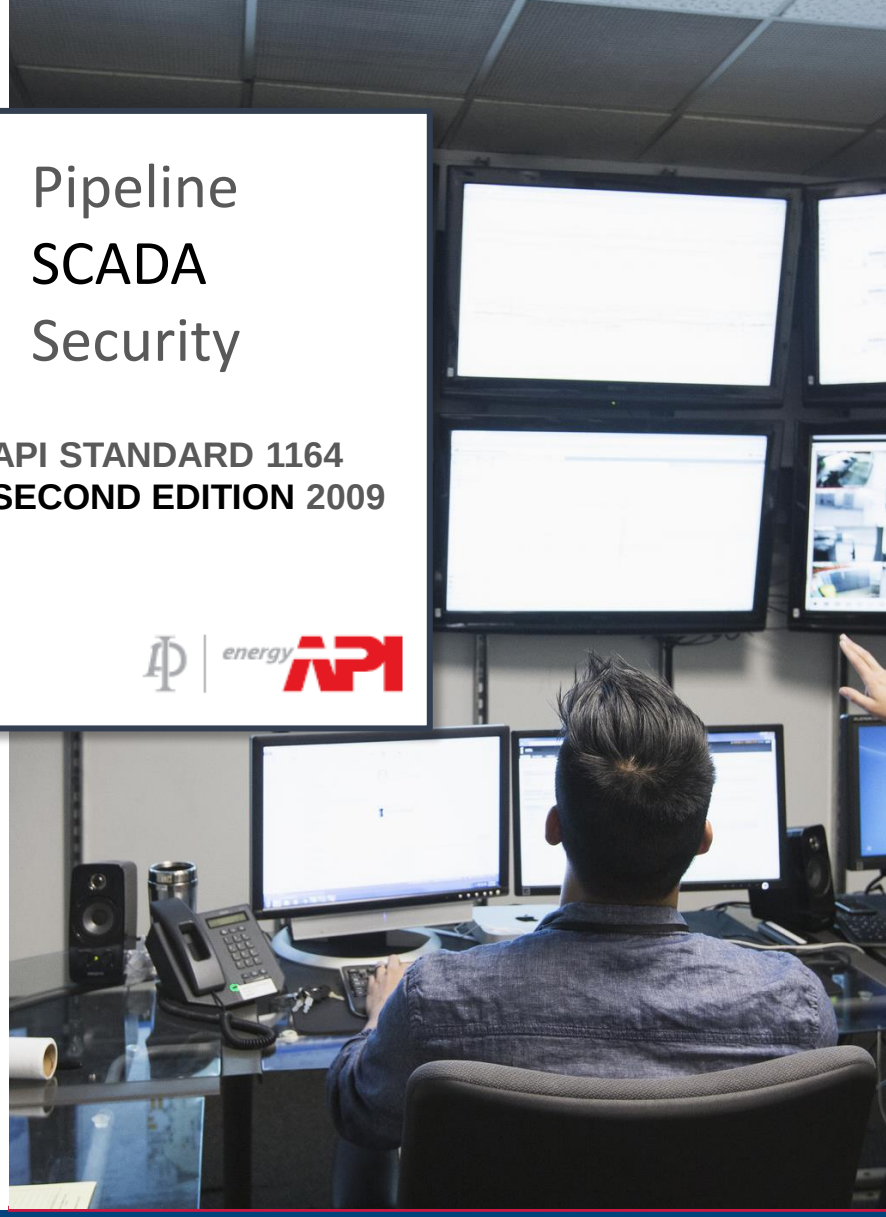
API

USEA
United States Energy Association

Rationale

Why this standard at this time?

- API Standard 1164 2nd Edition (2009):
  - Not widely adopted by industry .
  - Limited in scope (SCADA only).
  - Not materially revised during the last review cycle.
- Evolution of vulnerability and threat landscape (security risk).
  - SCADA protection alone ≠ Robust Defense-in-depth Strategy.
  - Entire control systems environment must be protected.
  - All stakeholders, including supply chain, must actively participate.
  - Ever increasing cybersecurity risks require a systematic approach for program governance and maturity.



Overview of 3rd Edition

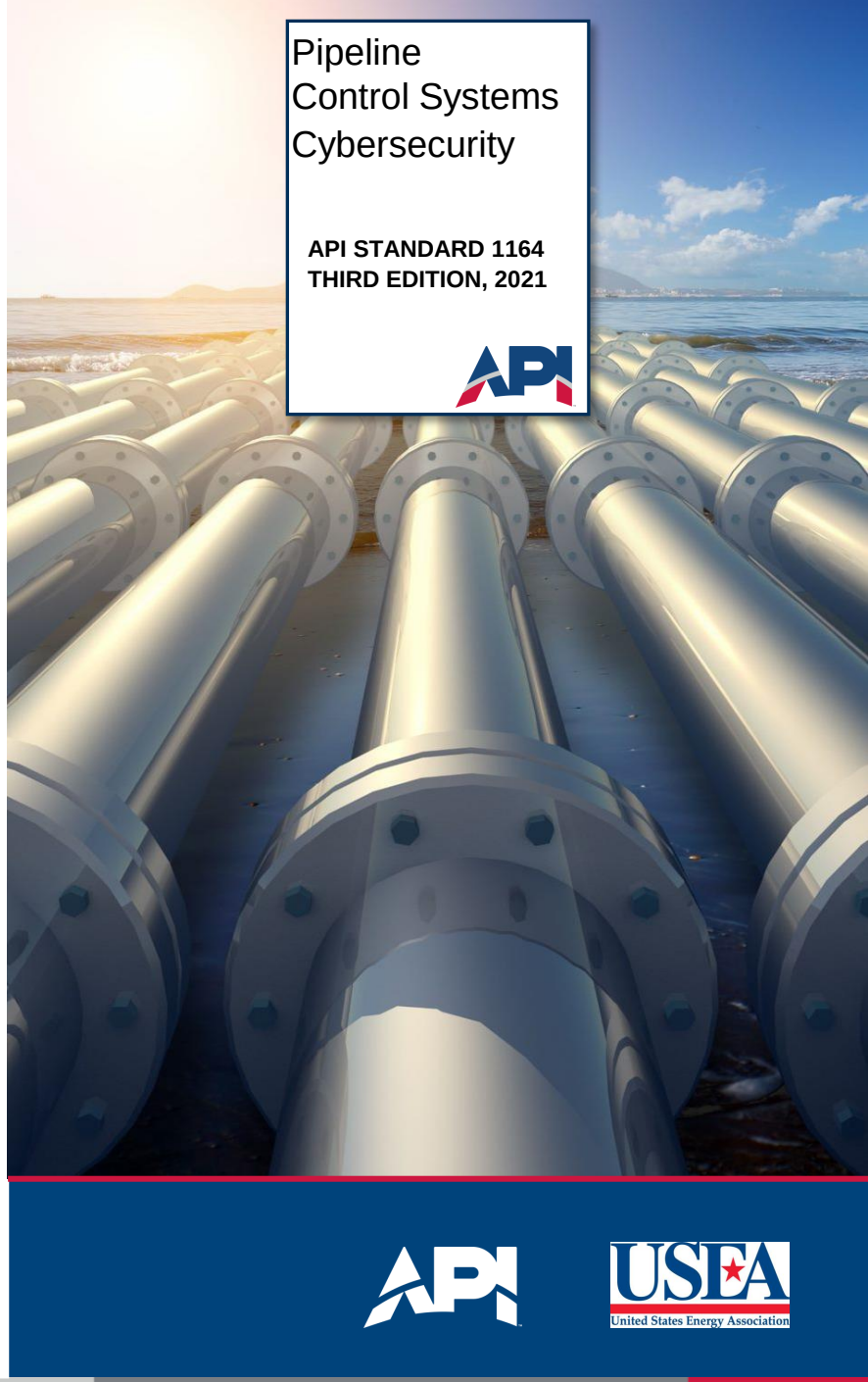
API

USEA
United States Energy Association

Scope

API 1164 3rd Edition:

- Complete re-write of the standard.
- Based on industry accepted cybersecurity standards (NIST CSF, NIST 800-53, NIST 800-82, ISA/IEC 62443).
- Focuses on pipeline specific control system (OT) security.
- Establishes management system for advancing program maturity
- Requires RISK-BASED implementation.

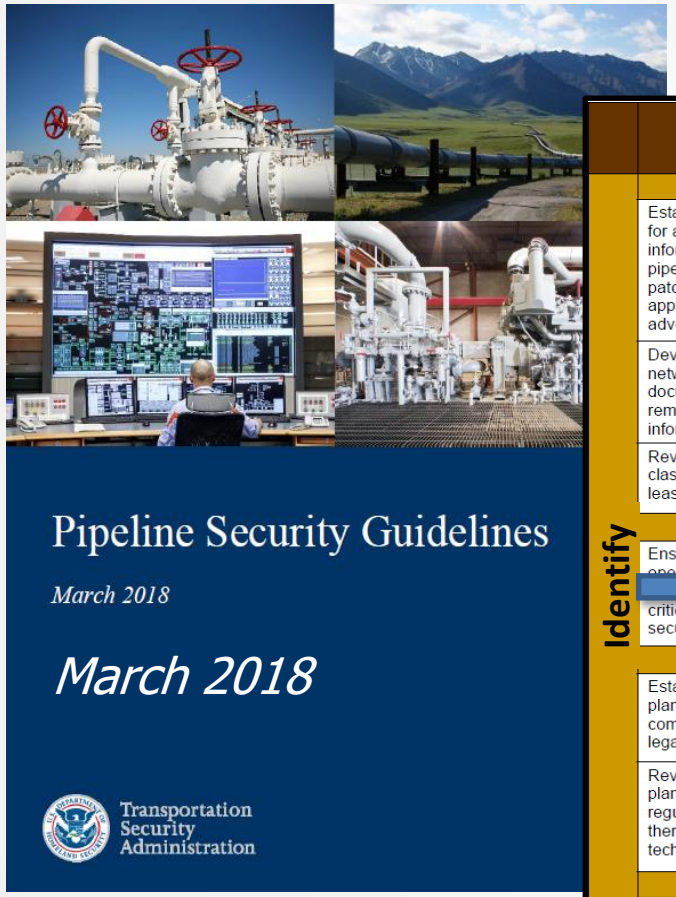


Standard 1164 3rd Edition
From Creation to Publication

API

USEA
United States Energy Association

March 2018 - TSA Aligned Cyber Objectives to NIST Framework:



	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. 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 Cyber Security Framework (CSF)

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

USEA United States Energy Association

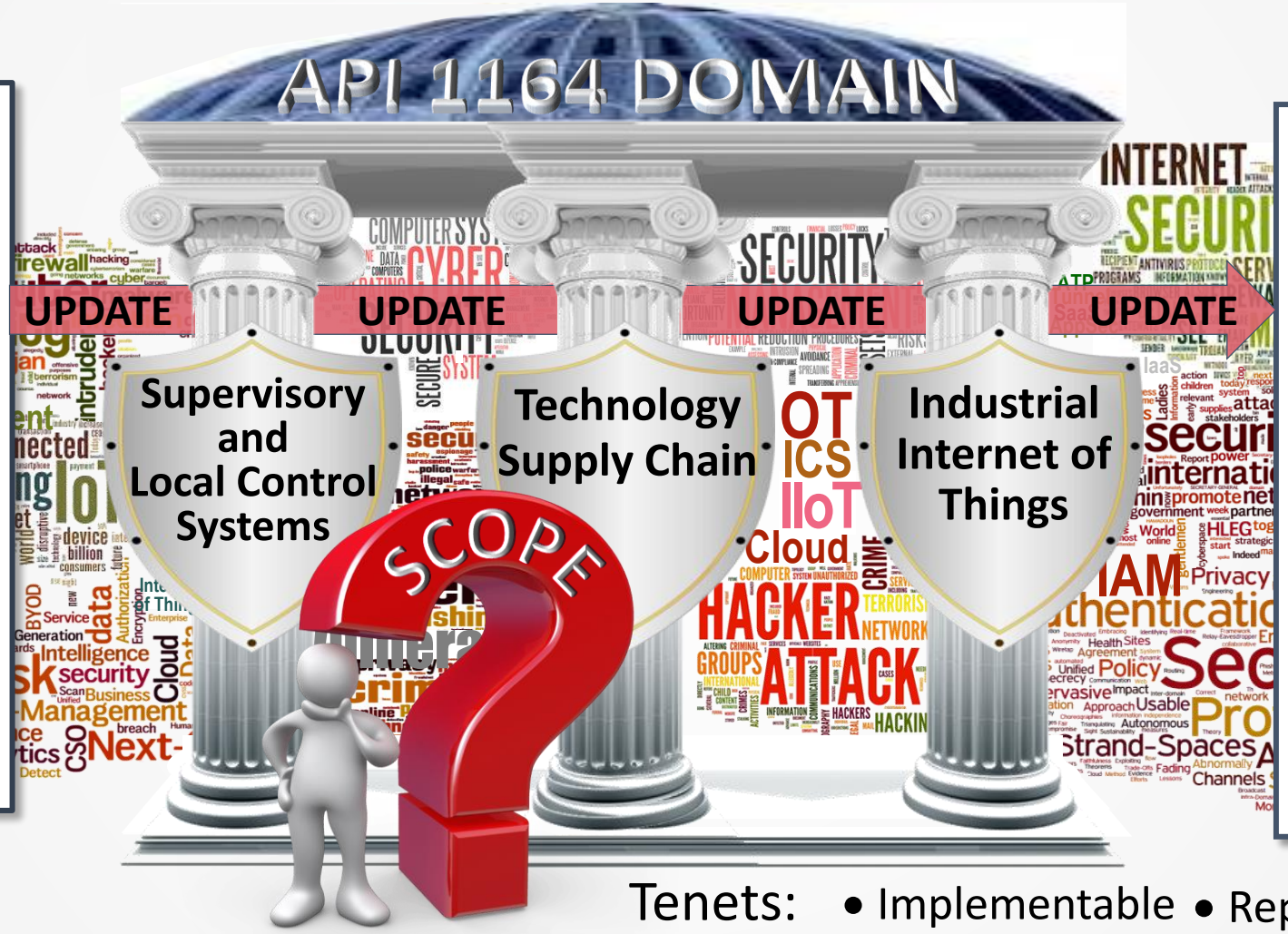
API

2 Months later, May 2018 – API Hosts 1st API 1164 Update Meeting

But to what depth and breadth of coverage?

Pipeline
SCADA
Security

API STANDARD 1164
SECOND EDITION 2009



Pipeline
Control Systems
Cybersecurity

API STANDARD 1164
THIRD EDITION

American Petroleum Institute

Tenets: • Implementable • Repeatable • Measurable

USEA United States Energy Association

Picking a Domain Base: Digital Technology Security Priorities

Definition: OT Essential Function:

Capability required to maintain health, safety, environment and availability for the equipment under control.

The **OT Cybersecurity Tenet:**

A security measure shall not adversely affect essential functions unless supported by a risk assessment.

USEA United States Energy Association

API

Why IAC Cybersecurity for Pipelines is Highly Important: Security = Safety

Definition: OT Essential Function:
Capability required to maintain health, safety, environment and availability for the equipment under control.

The **OT Cybersecurity Tenet:**
A security measure shall not adversely affect essential functions unless supported by a risk assessment.

	Pipeline Business Objectives	Manage cybersecurity risks that can…
1	**Maintain Human Health and Safety**	adversely impact human safety
2	**Maintain Environmental Safety**	adversely impact the environment
3	**Maintain Property Safety**	negatively impact the safety to physical
4	**Maintain Operational Capability**	adversely affect services and products delivery, including critical infrastructure
5	**Maintain Compliance Posture**	adversely impact a compliant posture with regulatory, legal, and corporate policy
6	**Maintain Reputation**	adversely affect the company's reputation or generate negative publicity

USEA United States Energy Association

API

Governance to Framework to Depth and Breadth Scope: ToC

TSA Pipeline 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. 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 results in the system being recognized as a 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.	

TSA Security Measures are 1164 Requirements

NIST CSF Core

Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Access Control
	Awareness Training
	Data Security
	Information Protection
	Maintenance
	Protective Technical Security Solutions
Detect	Anomaly and Event Detection
	Continuous Monitoring
	Detection Process
Respond	Response Planning
	Coordinated Response Activities
	Response and recovery analysis
	Containment, Mitigation and Eradication
	Process Improvement by Lessons Learned
Recover	Planning Processes & Procedures
	Process Improvement by Lessons Learned
	Communicate Restoration to Stakeholders

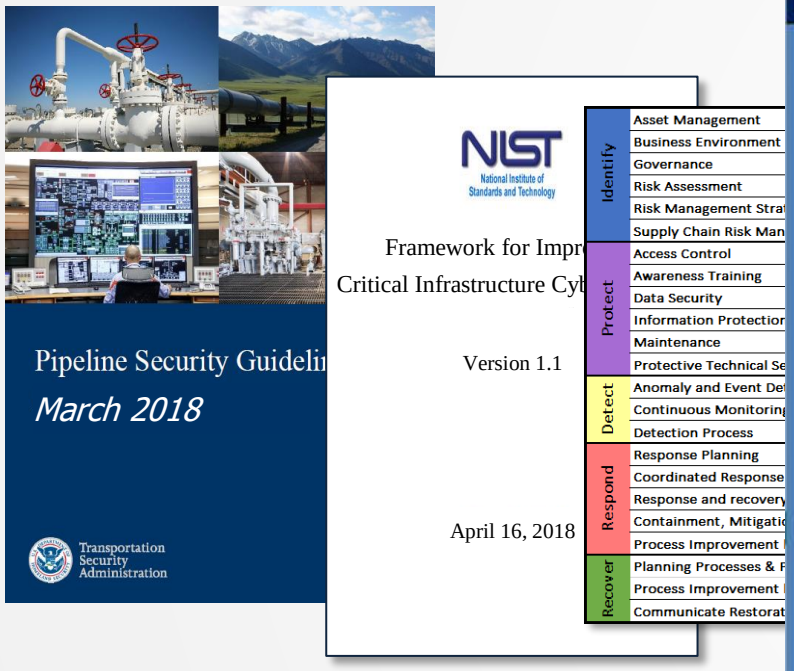
API 1164

- 6 **Identify** - ONG IAC Cybersecurity Requirements
  - 6.1 Governance
  - 6.2 Risk Management Strategy
  - 6.3 Business Environment
  - 6.4 Supply Chain Risk Management
  - 6.5 Risk Assessment
  - 6.6 Asset Management
- 7 **Protect** - ONG IAC Cybersecurity Requirements
  - 7.1 Access Control
  - 7.2 Awareness and Training
  - 7.3 Data Security
  - 7.4 Information Protection Processes / Procedures
  - 7.5 Maintenance
  - 7.6 Protective Technology
- 8 **Detect** - ONG IAC Cybersecurity Requirements
  - 8.1 Anomalies and Events
  - 8.2 Security Continuous Monitoring
  - 8.3 Detection Process
- 9 **Respond** - ONG IAC Cybersecurity Requirements
  - 9.1 Response Planning
  - 9.2 Communications
  - 9.3 Analysis
  - 9.4 Mitigation
  - 9.5 Improvements
- 10 **Recover** - ONG IAC Cybersecurity Requirements
  - 10.1 Recovery Planning
  - 10.2 Improvements
  - 10.3 Communications

USEA United States Energy Association

API

Cybersecurity Frameworks ≠ Security Controls nor Requirements

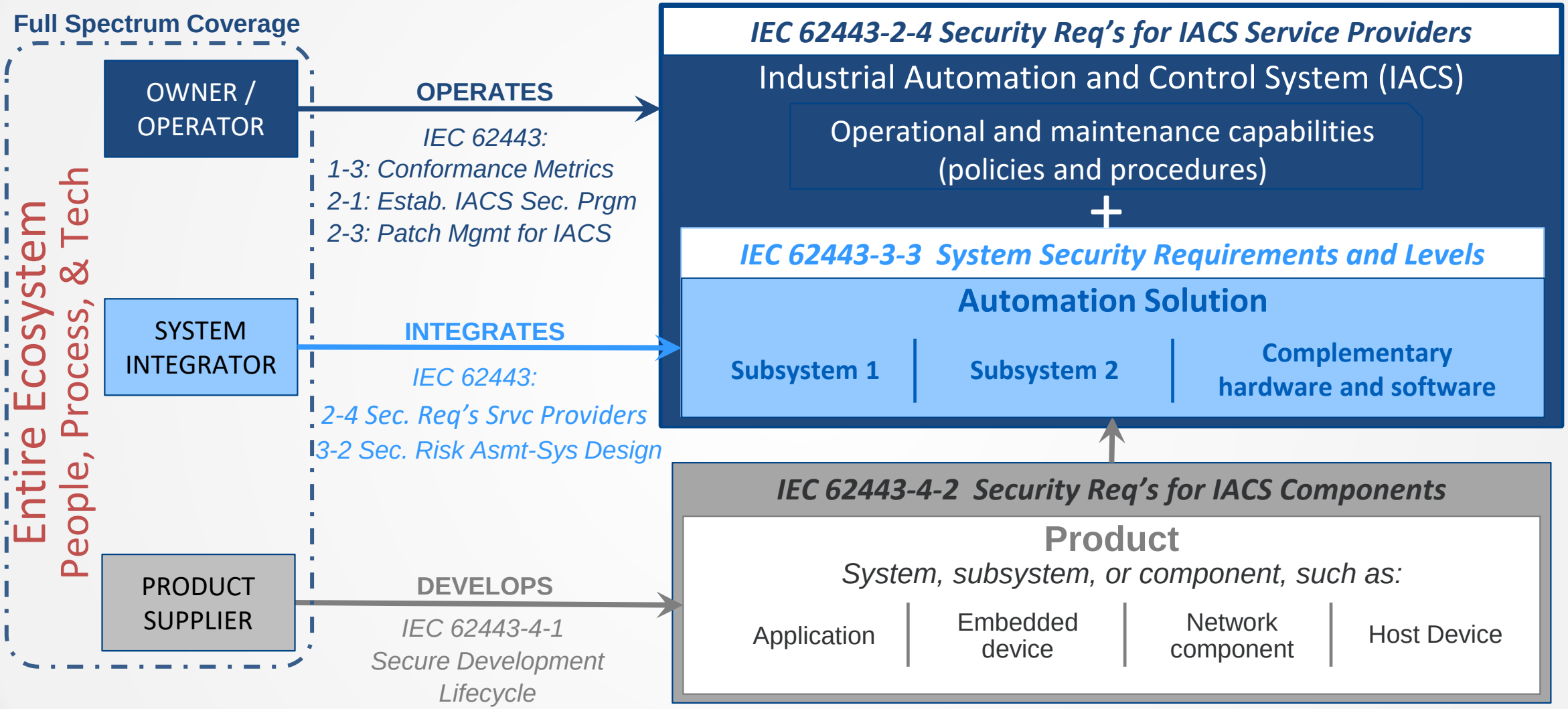


Funct.	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4 CM-8**
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4 CM-8**
		ID.AM-3: Organizational communication and data flows are mapped	· **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8**
		ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4 AC-20, SA-9**
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· COBIT 5 APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14**
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	· COBIT 5 APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

USEA United States Energy Association

API

ISA/IEC 62443 – Components, Products, Solutions, Services, Operations

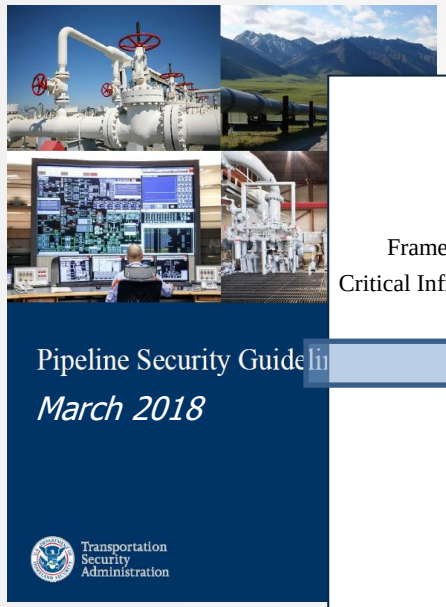


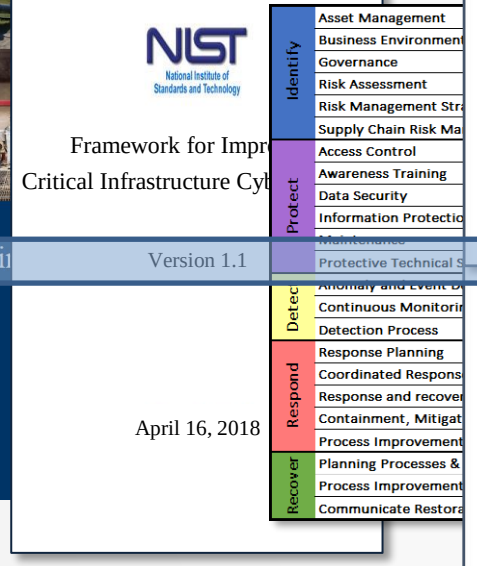
Cybersecurity Frameworks ≠ Security Controls nor Requirements

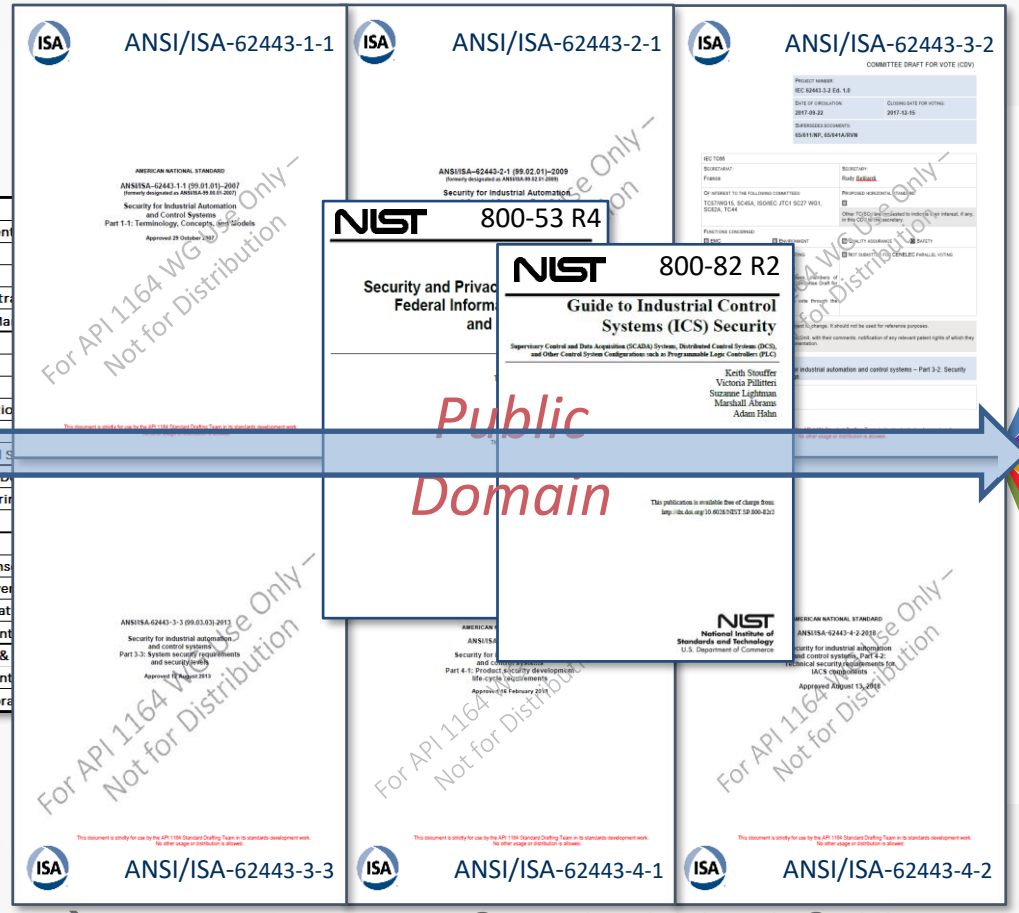
Developing Implementable, Repeatable, and Measurable Requirements

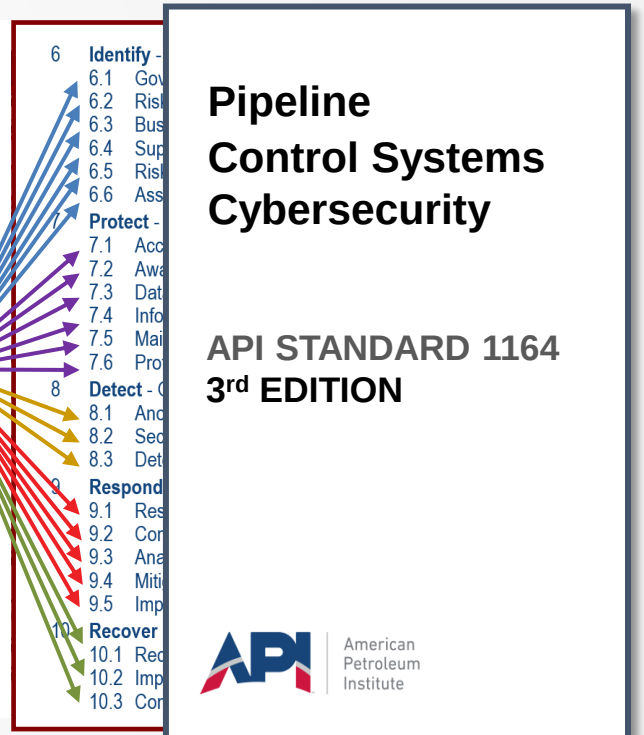
ISA Limited Use Permission

Tenets:
- Implementable
- Repeatable
- Measurable









Pipeline Control Systems Cybersecurity

API STANDARD 1164
3rd EDITION

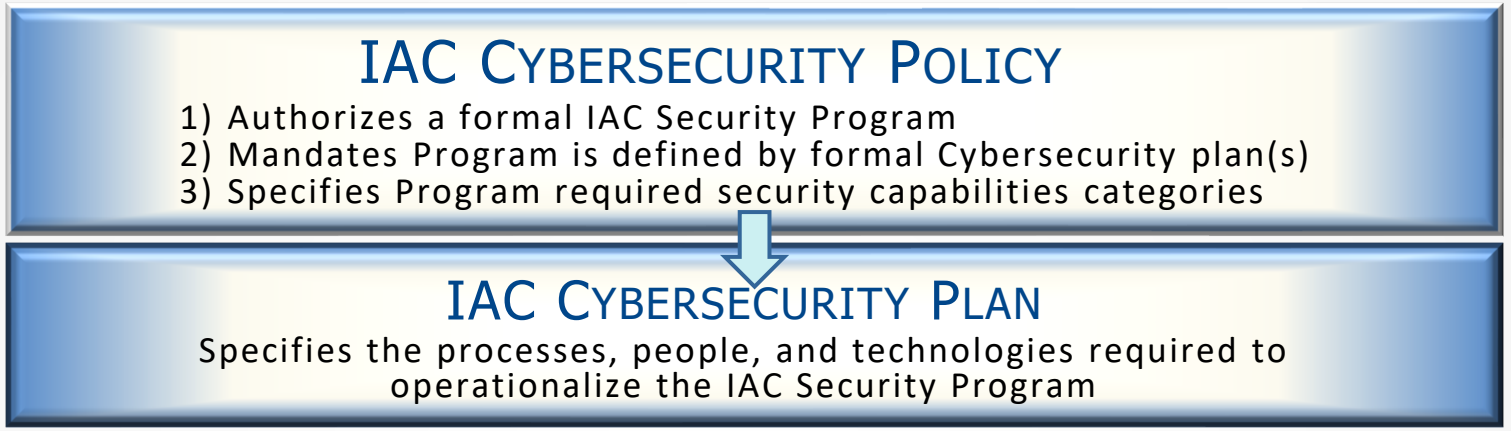
American Petroleum Institute

TSA Guidelines → NIST CSF → ISA 62443 & NIST 800-53 & 82 → API 1164

USEA United States Energy Association

API

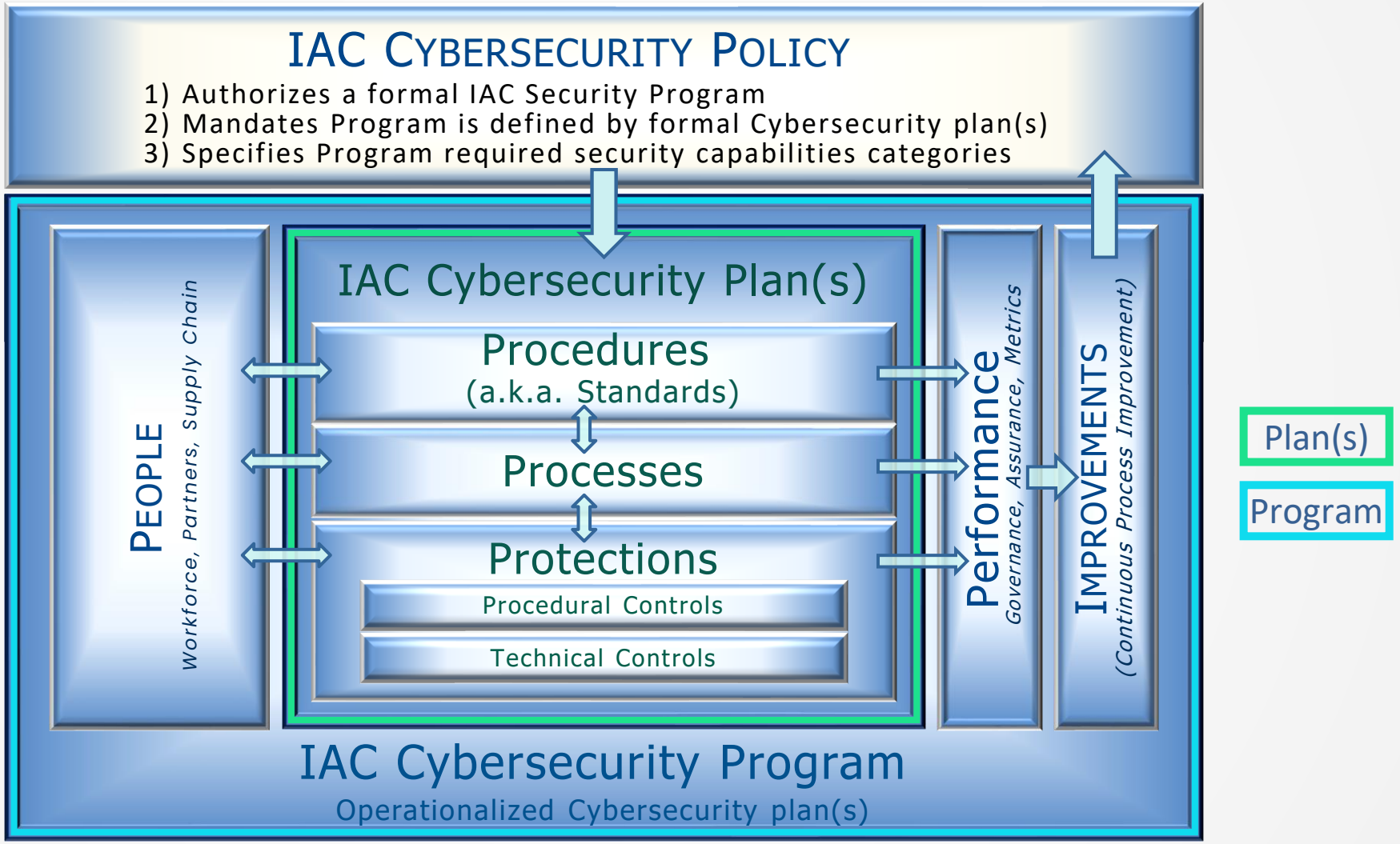
1164 Management System Governance Framework: Policy → Plan



Consistent with TSA Security Plan: Comprehensive Scope; Developed systematically; Risk-based

- ❑ Identify the primary and alternate security manager or officer responsible for executing and maintaining the plan;
- ❑ Document the company's security-related policies and procedures, methodologies used and timelines for conducting criticality assessments, risk assessments, and security vulnerability assessments;
- ❑ Reference other company plans, policies and procedures (e.g. business continuity, incident response / recovery);
- ❑ Be reviewed annually; updated based on findings from assessments, major modifications to the system;
- ❑ Be protected from unauthorized access based on company policy; and,

1164 Management System Governance Framework: Policy → Plan → Program



API 1164 3rd Edition

Basis of Cybersecurity Requirements Selection: Risk vs. Impact

Calculating Risk Score

Ref	Section	Issue Description	Consequence(s)	Control Measure(s)	Likelihood Score	Likelihood Rating	Impact Score	Impact Rating	Risk Score	Risk Rating
V6.2.2	Systems & Technology Failure	Risk Response: Outbound Internet Access Enabled from Device	• Disruption>Incapacitation • Usurpation > Misappropriation • Deception>Masquerade	• CM-1L Policy and Procedures • CM-2: Baseline Configuration • CM-3" Config Change Control • CM-7: Lease Functionality • CM-9: Config Mgmt. Plan • AC-3: Access Enforcement	7.2	?	5.9	?	42	?

Likelihood
X Impact
Risk

Threat Factors

Skill Required	Score	Motivation	Score	Opportunity	Score	Community Size	Score
Some Tech Skills	9	Opportunistic	8	Unauthenticated Basic Access	8	Authenticated Users	9
Advanced IAC / Security Penetration	1	Persistent	1	Authenticated Elevated Access	1	Security Administrators	1

Vulnerability Factors

Discoverability	Score	Exploitability	Score	Awareness	Score	Detectability	Score
Accidental	9	Easy	8	General Public Knowledge	9	Not Logged	9
Very Difficult	1	Multi-stage	1	Confidential	1	Logged w/ Automated Alerting	1

Threat Factors
X Vulnerability Factors
Potential Likelihood

Business Factors

Financial Damage	Score	Reputation Damage	Score	Non-Compliance	Score
Immeasurable	9	General Public - Corporate Image	10	Government Regulation	10
Negligible	1	Regional Customer	1	BU Standard	2

Technical Factors

Integrity Loss	Score	Availability Loss	Score	Confidentiality Loss	Score	Accountability	Score
Critical Function>Misuse (Malicious Logic)	9	DoS-Controller Equipment>Harm to Humans	10	Exfiltrate/Intercept Any> High-value IP	9	Unauthorized Access> Undetectable	10
Support Data>Corruption (Human Error)	1	Support Data Destruction>Restorable	2	Indirectly Inferred-Customer>Operational data	2	Unauthorized Access> Detectable - Short term	4

Business Factors
X Technical Factors
Potential Impact

USEA United States Energy Association

API

Risk vs. Impact

Risk Score vs. Rating

Rating Risk

Rating is Company Specific

Risk Score

Impact		Likelihood 1 Very Improbable	2 Improbable	3 Rare	4 Remote	5 Infrequent	6 Moderate	7 Likely	8 Very Likely	9 Frequent	10 Certain
1	Insignificant	1	2	3	4	5	6	7	8	9	10
2	Negligible	2	4	6	8	10	12	14	16	18	20
3	Marginal	3	6	9	12	15	18	21	24	27	30
4	Minor	4	8	12	16	20	24	28	32	36	40
5	Moderate	5	10	15	20	25	30	35	40	45	50
6	Significant	6	12	18	24	30	36	42	48	54	60
7	Major	7	14	21	28	35	42	49	56	63	70
8	Critical	8	16	24	32	40	48	56	64	72	80
9	Critical	9	18	27	36	45	54	63	72	81	90
10	Catastrophic	10	20	30	40	50	60	70	80	90	100

Risk Rating

Impact		Likelihood 1 Very Improbable	2 Improbable	3 Rare	4 Remote	5 Infrequent	6 Moderate	7 Likely	8 Very Likely	9 Frequent	10 Certain
1	Insignificant	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
2	Negligible	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
3	Marginal	Low	Low	Low	Low	Low	Low	Low	Low	Medium	Medium
4	Minor	Low	Low	Low	Low	Low	Low	Medium	Medium	Medium	Medium
5	Moderate	Low	Low	Low	Low	Medium	Medium	Medium	Medium	Medium	High
6	Significant	Low	Low	Low	Low	Medium	Medium	Medium	Medium	High	High
7	Major	Low	Low	Low	Medium	Medium	Medium	High	High	High	Critical
8	Critical	Low	Low	Low	Medium	Medium	Medium	High	High	Critical	Critical
9	Critical	Low	Low	Medium	Medium	Medium	High	High	Critical	Critical	Critical
10	Catastrophic	Low	Low	Medium	Medium	High	High	Critical	Critical	Critical	Critical

USEA United States Energy Association

API

Risk vs. Impact

Risk Rating vs. Response

Assessing Risk

Response is Company Specific

Ref	Section	Issue Description	Consequence(s)	Control Measure(s)	Likelihood Score	Likelihood Rating	Impact Score	Impact Rating	Risk Score	Risk Rating
V6.2.2	Systems & Technology Failure	Risk Response: Outbound Internet Access Enabled from Device	• Disruption>Incapacitation • Usurpation > Misappropriation • Deception>Masquerade	• CM-1L Policy and Procedures • CM-2: Baseline Configuration • CM-3" Config Change Control • CM-7: Lease Functionality • CM-9: Config Mgmt. Plan • AC-3: Access Enforcement	7.2	Likely	5.9	Significant	42	Medium

Score	Risk Rating
0	Low
21	Medium
30	Medium
35	Medium
49	High
60	High
65	Critical
70	Critical

Impact		Likelihood 1 Very Improbable	2 Improbable	3 Rare	4 Remote	5 Infrequent	6 Moderate	7 Likely	8 Very Likely	9 Frequent	10 Certain
1	Insignificant	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
2	Negligible	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
3	Marginal	Low	Low	Low	Low	Low	Low	Medium	Medium	Medium	Medium
4	Minor	Low	Low	Low	Low	Low	Medium	Medium	Medium	Medium	Medium
5	Moderate	Low	Low	Low	Low	Medium	Medium	Medium	Medium	Medium	High
6	Significant	Low	Low	Low	Medium	Medium	Medium	Medium	Medium	High	High
7	Major	Low	Low	Medium	Medium	Medium	Medium	High	High	High	Critical
8	Critical	Low	Low	Medium	Medium	Medium	Medium	High	High	Critical	Critical
9	Critical	Low	Low	Medium	Medium	Medium	High	High	Critical	Critical	Critical
10	Catastrophic	Low	Low	Medium	Medium	High	High	Critical	Critical	Critical	Critical

Risk Responses: ☑ Treat ☑ Terminate ☑ Transfer ☑ Tolerate

🚫 Risk-based Bright-line Rules are not appropriate for a Standard

USEA United States Energy Association API

How to Determine Impact

API 780: SRA Methodology – Event Consequences

5 Levels of Impact Severity

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

API STANDARD 780

energy API
AMERICAN PETROLEUM INSTITUTE

ANSI

1	Health	a) Possibility of minor injury on-site; no fatalities or injuries anticipated off site.
	Environment	b) No environmental impacts.
	Property	c) Up to $X loss in property damage.
	Operations	d) Very short-term (up to X weeks) business interruption/expense.
	Reputation	e) Very low or no impact or loss of reputation or business viability; mentioned in local press.
2	Health	a) On-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities or injuries anticipated off site.
	Environment	b) Minor environmental impacts to immediate incident site area only, less than X year(s) to recover.
	Property	c) $X to $X loss in property damage.
	Operations	d) Short-term (>X week to Y months) business interruption/expense.
	Reputation	e) Low loss of reputation or business viability; query by regulatory agency; significant local press coverage.
3	Health	a) Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off site.
	Environment	b) Impact on-site and/or minor off-site impact, Y year(s) to recover.
	Property	c) Over $X to $X loss in property damage.3
	Operations	d) Medium-term (Y to Z months) business interruption/expense.
	Reputation	e) Medium loss: reputation/business viability; attention of regulatory agencies; national press coverage.
4	Health	a) Possibility of X to Y on-site fatalities; possibility of off-site injuries.
	Environment	b) Very large impact on-site and/or large off-site impact, between Y and Z years to recover.
	Property	c) Over $X to $X loss in property damage.
	Operations	d) Long-term (X to Y years) business interruption/expense.
	Reputation	e) High loss: reputation/business viability; prosecution by regulator; extensive national press coverage.
5	Health	a) Possibility of any off-site fatalities from large-scale toxic or flammable release; possibility of multiple on-site fatalities.
	Environment	b) Major impact on-site and/or off site (e.g. large-scale toxic contamination of public waterway), more than XX years/poor chance of recovery.
	Property	c) Over $X loss in property damage.
	Operations	d) Very long-term (>X years) business interruption/expense; large-scale disruption to the national economy, public or private operations; loss of critical data.
	Reputation	e) Very high loss of reputation or business viability; international press coverage.

USEA United States Energy Association

API

780 Safety Event Consequences to 1164 Business Objective Impact Levels

API 780: SRA Methodology Event Consequences

API SRA Methodology		
	Description	Ranking
a)	Possibility of minor injury on-site; no fatalities or injuries anticipated off site.	1
b)	No environmental impacts.	
c)	Up to $X loss in property damage.	
d)	Very short-term (up to X weeks) business interruption/expense.	
e)	Very low or no impact or loss of reputation or business viability; mentioned in local press.	
a)	On-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities o…es anticipated off site.	2
b)	Minor environmental impacts to immediate incident site area only, less than X year(s) to recover.	
c)	$X to $X loss in property damage.	
d)	Short-term (>X week to Y months) business interruption/expense.	
e)	Low loss of reputation or business viability; query by regulatory agency; significant local press coverage.	
a)	Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off site.	3
b)	Environmental impact on-site and/or minor off-site impact, Y year(s) to recover.	
c)	Over $X to $X loss in property damage.	
d)	Medium-term (Y to Z months) business interruption/expense.	
e)	Medium loss of reputation or business viability; attention of regulatory agencies; national press coverage	
a)	Possibility of X to Y on-site fatalities; possibility of off-site injuries.	4
b)	Very large environmental impact on-site and/or large off-site impact, between Y and Z years to recover.	
c)	Over $X to $X loss in property damage.	
d)	Long-term (X to Y years) business interruption/expense.	
e)	High loss of reputation or business viability; prosecution by regulator; extensive national press coverage.	
a)	Possibility of any off-site fatalities from large-scale toxic or flammable release; possibility of multipl…te fatalities.	5
b)	Major environmental impact on-site and/or off site (e.g. large-scale toxic contamination of public waterwa…re than XX years/poor chance of recovery.	
c)	Over $X loss in property damage.	
d)	Very long-term (>X years) business interruption/expense; large-scale disruption to the national economy…or private operations; loss of critical data.	
e)	Very high loss of reputation or business viability; international press coverage.	

5 Levels of Impact Severity

API 1164: Business Objective Impact Severity Levels

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

USEA United States Energy Association

API

Determining Threat Protections for Business Objective Impact Severity Levels

ISA/IEC 62443 – Threat Protection Security Levels

5 Levels of Security Capability

Sec. Lvl	Threat Protection Objective
SL 0	No specific requirements or security protection necessary
SL 1	Protect against casual or coincidental security violation
SL 2	Protect against intentional security violation using simple means with low resources, generic skills and low motivation.
SL 3	Protect against intentional security violation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
SL 4	Protect against intentional security violation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

Business Objective Impact Severity Levels to Threat Protection Profiles

API 1164: Threat Protection Objectives and IAC Cybersecurity Profiles

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

API 1164: Business Objective Impact Severity Levels

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

USEA United States Energy Association

API

Tying It All Together

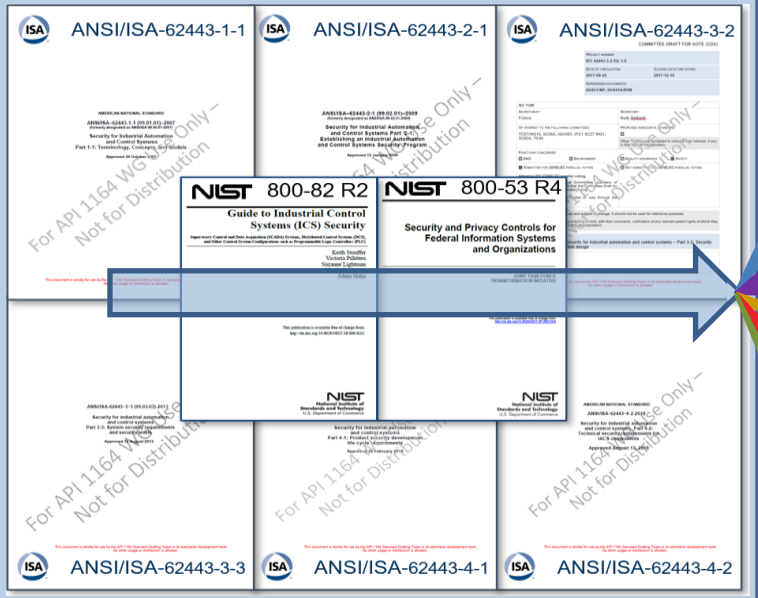
Industry Recognized Supporting Standards

NIST CSF
Drives critical infrastructure scope and high-level Cybersecurity Program capabilities

Function	Category	Subcategory
Identify	Asset Management	
	Business Environment	
	Governance	ID.GV-1: Organizational cybersecurity policy is established and communicated
	Risk Assessment	
	Risk Management Strategy	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
	Supply Chain Risk Management	
Protect	Access Control	
	Awareness Training	
	Data Security	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
	Information Protection	
	Maintenance	
	Protective Technical Security Solutions	
Detect	Anomaly and Event Detection	
	Continuous Monitoring	
	Detection Process	
Respond	Response Planning	
	Coordinated Response Activities	
	Response and recovery analysis	
	Containment, Mitigation and Eradicatio	
	Process Improvement by Lessons Learn	
Recover	Planning Processes & Procedures	
	Process Improvement by Lessons Learn	
	Communicate Restoration to Stakehold	

Industry Recognized Standards leveraged for detailed requirements

(NIST CSF Informative References plus 5 additional standards)



API Standard 1164 3rd Edition

IAC Cybersecurity Policy

1) Authorizes a formal IAC Security Program
2) Mandates Program is defined by a formal Plan
3) Specifies capability categories for the Program

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

Mgmt. System Framework

6 **Identify** - ONG IAC Cybersecurity Requirements
- 6.1 Governance
- 6.2 Risk Management Strategy
- 6.3 Business Environment
- 6.4 Supply Chain Risk Management
- 6.5 Risk Assessment
- 6.6 Asset Management

7 **Protect** - ONG IAC Cybersecurity Requirements
- 7.1 Access Control
- 7.2 Awareness and Training
- 7.3 Data Security
- 7.4 Information Protection Processes / Procedures
- 7.5 Maintenance
- 7.6 Protective Technology

8 **Detect** - ONG IAC Cybersecurity Requirements
- 8.1 Anomalies and Events
- 8.2 Security Continuous Monitoring
- 8.3 Detection Process

9 **Respond** - ONG IAC Cybersecurity Requirements
- 9.1 Response Planning
- 9.2 Communications
- 9.3 Analysis
- 9.4 Mitigation
- 9.5 Improvements

10 **Recover** - ONG IAC Cybersecurity Requirements
- 10.1 Recovery Planning
- 10.2 Improvements
- 10.3 Communications

P3 Extended Profile

P2 Enhanced Profile

P1 Baseline Profile

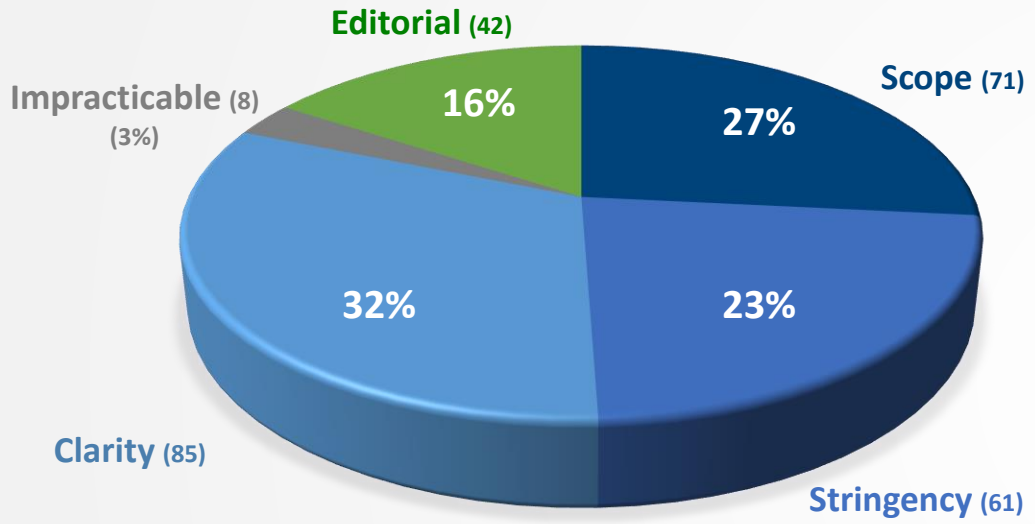
Detailed req's allocated to 3 Protection Profiles based on impact to business objectives.

The higher the impact the higher the protection to defend against more advanced threats

API 1164 3rd Edition Balloted in 1Q 2021

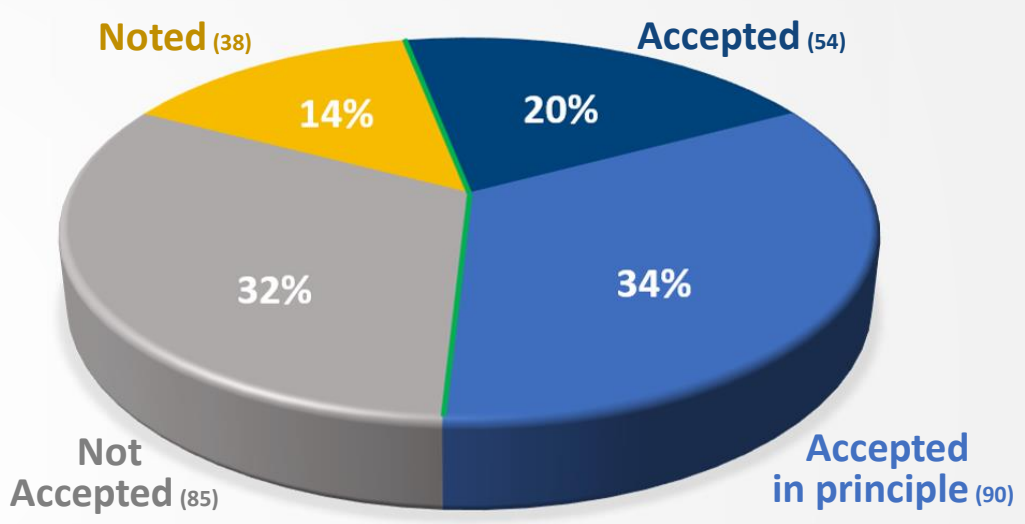
Balloted Standard – Public Comment Review and Resolution

COMMENT FOCUS



Scope:	Inappropriate scope (too much or too little).
Stringency:	Requirement applies too much rigor for the security profile to which it is assigned, or is too burdensome to be implemented.
Clarity:	Insufficiently clear, inconsistent, or poorly written (wording / sentence structure)
Impracticable:	Too general or insufficiently specific to be actionable
Editorial:	Grammar, misspellings, punctuation, etc.

COMMENT DISPOSITION



Accepted:	Verbatim change made.
Accepted in Principle:	Changed to reflect the principle of the accepted comment but not exactly as suggested by the commenter).
Not Accepted:	No revision in-line with comment. Some changes may have been applied for clarity to address comment premise misunderstanding or misconception.
Noted:	Comment logged for future review.

USEA United States Energy Association

API

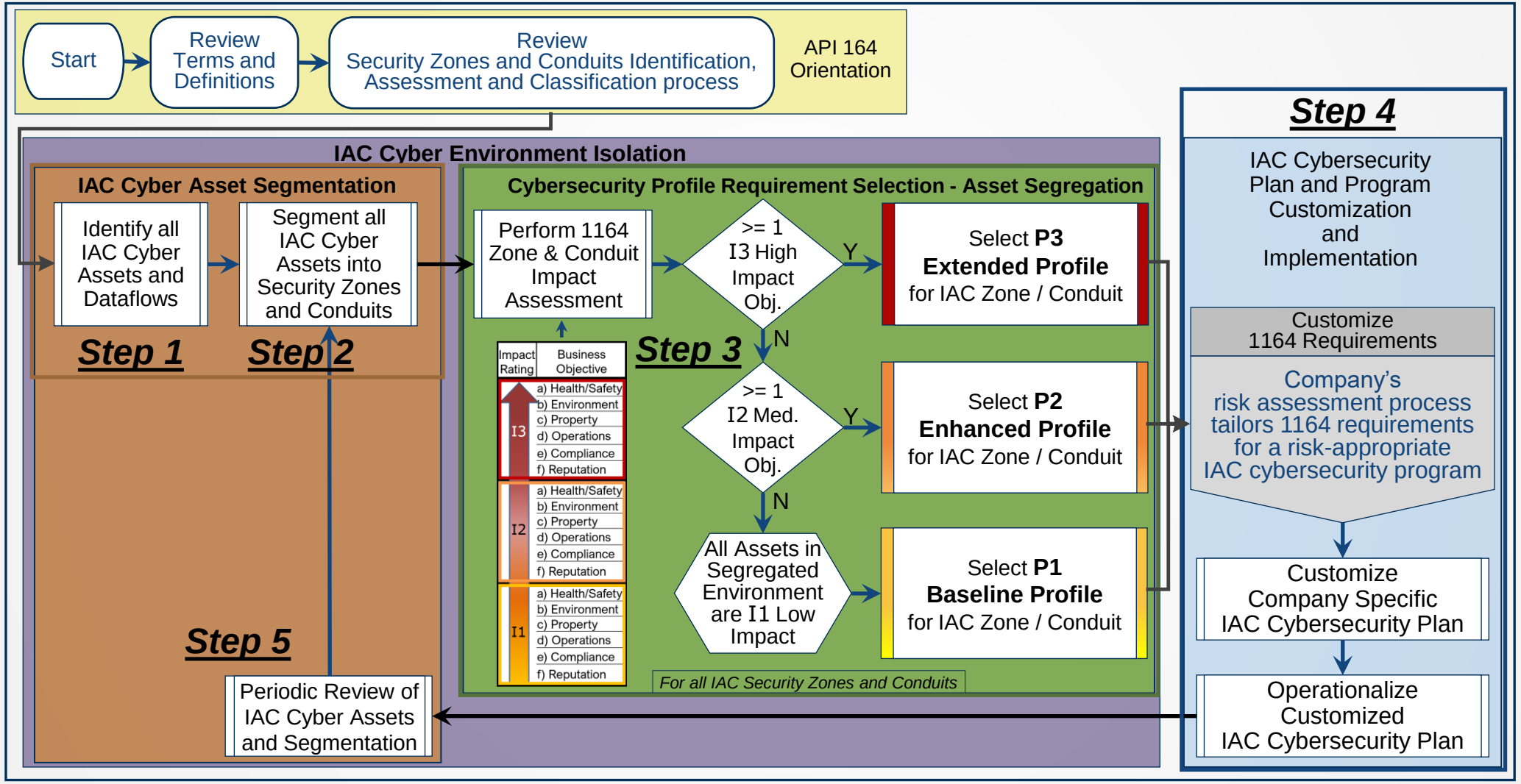
- **Not One and Done**

Maturing 1164 IAC Cybersecurity Program

Maturing Standard 1164 3rd Edition

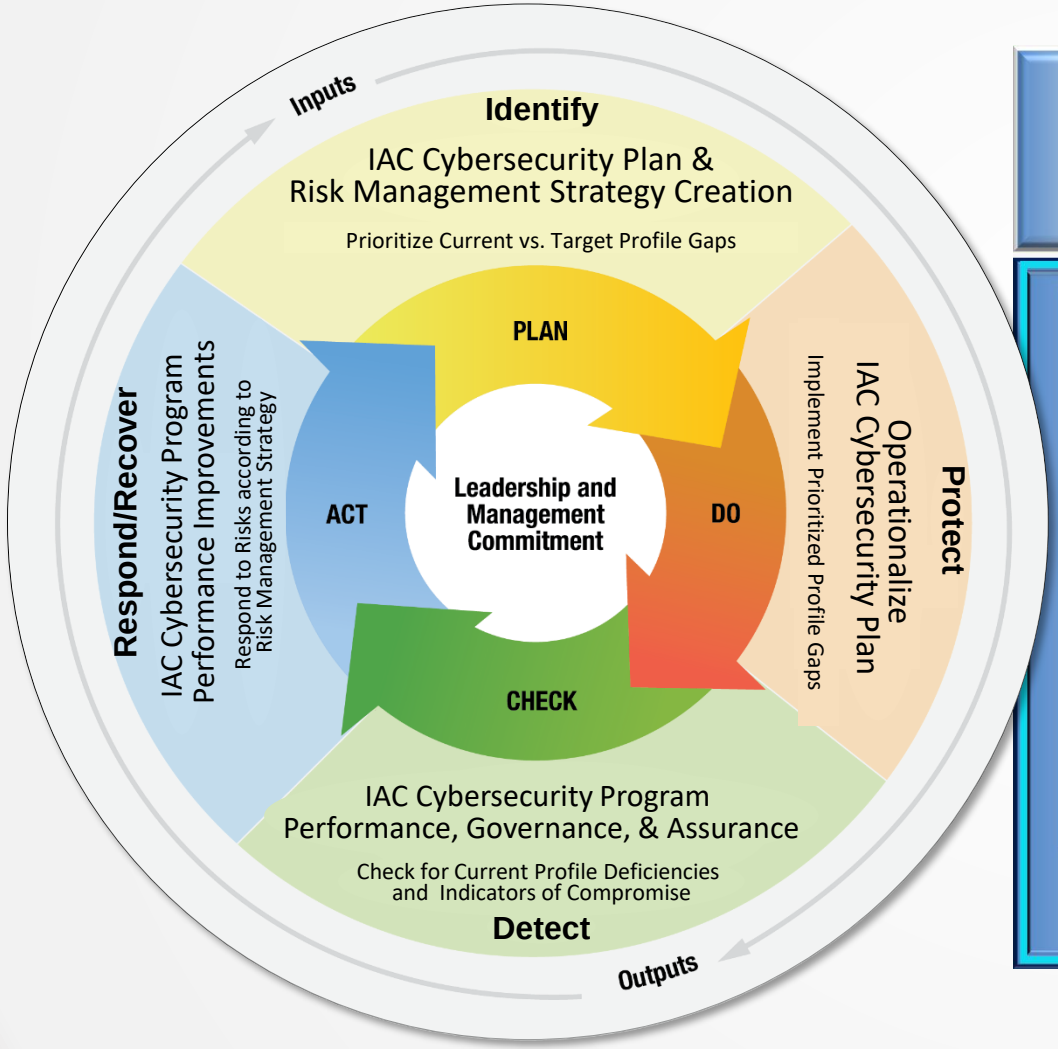
API 1164 Profile Requirement Selection and Plan Implementation

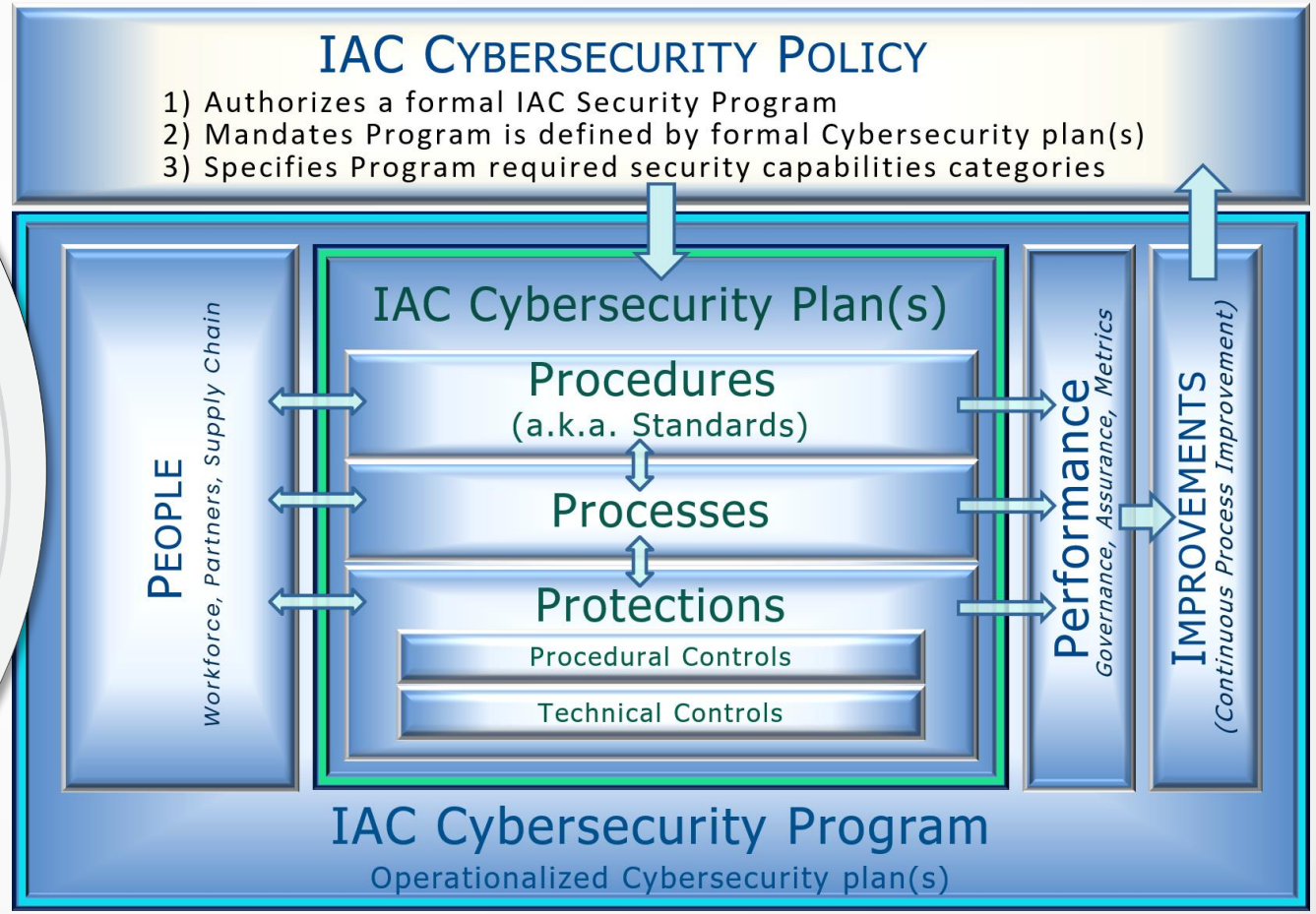
5 Steps: IAC Cybersecurity Plan and Program Maturation



API 1164 Profile Requirement Selection and Plan Implementation

Management System Framework: Plan and Program Maturation

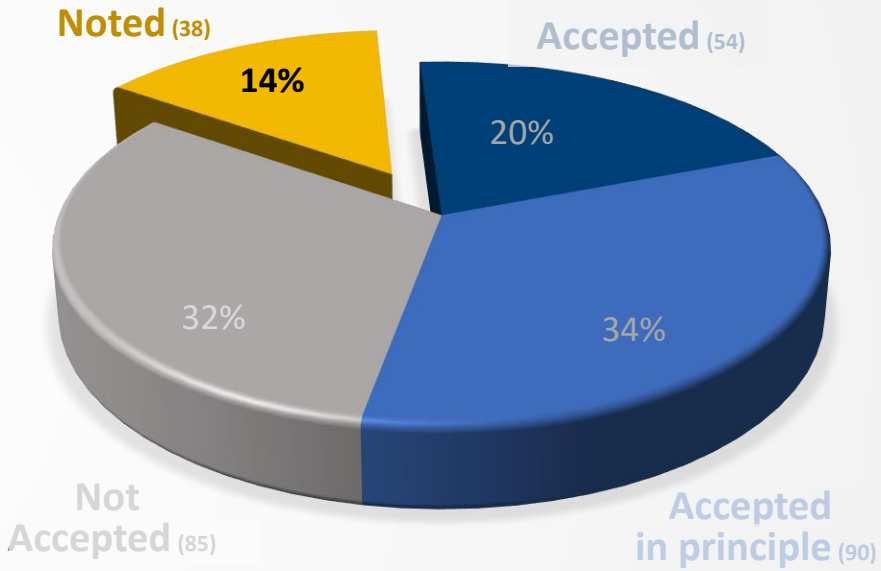




API Standards Review Cycle: Periodic vs. Continuous Maintenance

- Periodic Maintenance Cycle
  - Every 5 Years (typical) or
  - Significant change/event germane to Standard's domain
  - If no substantive changes, balloted for reaffirmation
- Continuous Maintenance Cycle Process
  - Enables frequent consideration of proposed updates.
  - Updates considered via regularly scheduled TG meetings.
  - Comments under consideration
    - "Noted" comments from balloting process
    - Comments collected during final review (recirculation process)
    - Feedback provided on implementation of new edition
    - New comments based on changing circumstances/scenarios
  - Updates approved via API's Standards Balloting Process.
  - Updates issued as addenda to Standard.

COMMENT DISPOSITION



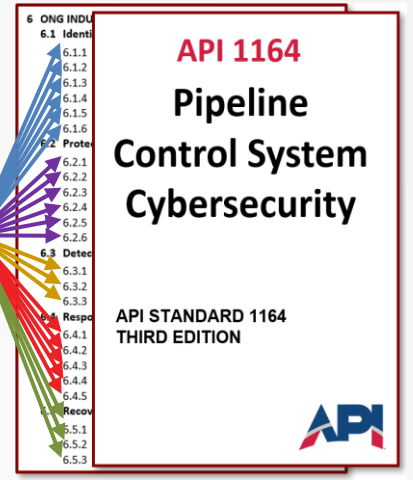
Noted: Comment logged for future review.

API 1164 – Broad Industry Consensus Standard

2 Months after
TSA Pipeline Security Guidelines V3,
API Hosts 1st meeting
to rewrite API 1164

API published new
Broad Consensus Standard
for Pipeline Control System
Cybersecurity

3+ Years in the making



API AGA INGAA

3 Industry Trade Organizations

3 Federal and State Agencies

50+ Companies

80+ Industry Experts

12,000+ Hours of effort

- ✓Covers all NIST CSF Functions - Subcategories
- ✓Extends beyond NIST CSF Informative Refs.
- ✓Based off international standards
- ✓Covers cyber supply chain
- ✓Provides 3 security protection profiles
- ✓Addresses 3 levels of potential impacts
- ✓Aligns to 6 common pipeline business objectives
- ✓Requires risk-based implementation
- ✓Is tailorable for company specific risk
- ✓Kept current with continuous maintenance

USEA United States Energy Association

API

Special Thanks

To these organizations who contributed to the development and release of API 1164, 3rd Edition

American Gas Association

Interstate Natural Gas Association of America

Question & Answer

Please Use the Chat Function to Enter Your Question

United States Energy Association