International Association of Drilling Contractors (IADC)

Guidelines for Minimum Cybersecurity Requirements for Drilling Assets

EXECUTIVE SUMMARY

The rate of cybersecurity attacks and the attacks' level of sophistication and organization are increasing. In 2014 – according to the US Department of Homeland Security (DHS) - 53% of all cyber-attacks on critical infrastructure targeted the energy industry, and 30% of the attacks succeeded in breaching the security systems that were in place. In 2015, DHS recorded more than 9 cyber-attacks per day that targeted the energy industry.

Cyber attacks represent a significant financial and environmental risk to firms with Oil and Gas (O&G) operations. The attacks may: (1) disrupt or shut down operations, (2) cause environmental or human damage or impact, (3) steal information, (4) impact production schedules, (5) increase operational costs, (6) expose the organization´s to legal liabilities, and (7) damage the organization´s reputation. As automation and Internet connectivity of offshore drilling assets increase, the O&G industrial control systems become more susceptible to cyber attacks, but also to accidental and non-malicious user behavior.

The increase in threats against critical infrastructure prompted the United States government to strengthen and expand regulations of cybersecurity for critical infrastructure, including the energy and O&G industry. In February 2013, President Obama issued Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity." EO 1363 directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The result of the directive, the "NIST Cybersecurity Framework" was published in February 2014. The Framework embodies international and regional cybersecurity regulations and standards, and guides compliance through recommended best practices. By defining five core cybersecurity functions: Identify, Protect, Detect, Respond and Recover, the Framework provides a basis for a holistic cybersecurity strategy. The framework is internationally recognized as a de-facto cybersecurity best practice.

This Document specifies requirements for cybersecurity solutions for O&G drilling assets that derive from the NIST Cybersecurity Framework and apply to the Operational Technology (OT), Industrial Controls Systems (ICS) and Automation systems found on drilling assets. This Document also summarizes the evolution of domestic and international cybersecurity regulations and standards put forward by governments and standards bodies. And finally, this Document describes how the NIST Cybersecurity Framework aligns with international and regional cybersecurity standards and regulations.

TABLE OF CONTENTS

1 OVERVIEW OF CYBERSECURITY REGULATORY ENVIRONMENT

O&G drilling assets have specific cybersecurity requirements stemming from the inherent nature of the industry, the increasing adoption of existing standards - both generic and specific - and the growing trend of regulation of the industry regarding cybersecurity. This section examines the U.S.A., E.U. and UK initiatives that are relevant for drilling cybersecurity.

1.1 General Infrastructure Cybersecurity Requirements and Standards

The United States of America is leading a national initiative to secure its critical infrastructure and is coordinating these efforts internationally with professional associations such as the American Petroleum Institute (API) and the International Association of Drilling Contractors (IADC), as well as with international standards organizations including the International Organization for Standardization (ISO) and the International Society of Automation (ISA). The resulting standards, whether originating from the U.S.A. or elsewhere, overlap in their purpose, scope, and audience and have more commonalities than differences.

The overarching goal is the same across all standards: *To protect critical infrastructure*. The U.S.A. and the E.U. define critical infrastructure similarly:

- The United States Patriot Act defines critical infrastructure as, *"…systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*"
- The European Commission defines critical infrastructure as *"… an asset, system, or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which could have a significant impact on a Member State as a result of the failure to maintain those functions."*[1]

The two definitions both refer to systems and assets and their criticality for the safety, health, and well-being of their respective citizens. The salient difference between the two is that the U.S.A. explicitly includes virtual systems and assets within their definition of critical infrastructure so that one could argue this definition encompasses intangible assets such as intellectual property.

1.2 The United States of America (U.S.A.)

The U.S.A. has established policies and procedures for protecting critical infrastructure from Presidential Policy Directives (PPD) and Executive Orders (EO) issued by Presidents Bill Clinton, George W. Bush, Barack Obama and Donald Trump. It is important to review the PPDs and EOs in their totality over the past 15 years.

Presidential Decision Directive 63: President Clinton established the Commission on Critical Infrastructure Protection (CIPP) which led to the release of Presidential Decision Directive 63 that (1)

[1] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

established the first 15 critical infrastructure sectors, and (2) established Information Sharing and Analysis Centers (ISACs) to coordinate federal, state, local, and private sector efforts. These sectors and the ISACs remain in effect today.

Executive Order 13231: Responding to the 9/11 attacks, on October 16, 2001, President George W. Bush issued Executive Order 13231 establishing the President's Critical Infrastructure Protection Board (CIPB) and the National Infrastructure Advisory Council (NIAC)[2]. This represented a major shift toward a more definitive policy direction than PDD-63. This EO stated three goals: (1) Prevent cyber attacks against America's critical infrastructure; (2) Reduce national vulnerability to cyber attacks, and (3) Minimize damage and recovery time from cyber attacks that do occur.

The CIPB published "The National Strategy to Secure Cyberspace" to improve US critical infrastructure cybersecurity by first requiring federal agencies to incorporate best security practices and then using these best security practices as a "guide" for private industry. While PPD-63 encouraged a public—private partnership to reduce vulnerabilities, this EO was more direct in advocating for employing federal security practices in private industry.

The main objectives outlined in the Report were the following:

1. **Establish a national cyberspace response system** between the public and private sectors to analyze and warn; manage significant incidents; ensure business continuity; and share information.
2. **Establish a national cyberspace security threat and vulnerability reduction program** to reduce threats and identify/deter malicious actors; identify and remediate the critical infrastructure vulnerabilities that could cause the most damage; and develop new systems with less vulnerabilities.
3. **Establish a national security awareness and training program**.
4. **Secure governments' (federal, state, and local) cybersecurity**.
5. **Establish national security and international cyberspace security cooperation**.

The PCIPB coordinates the federal government's cyber infrastructure protection policy, while NIAC manages the "partnership of the public and private sectors in protecting information systems for critical infrastructures."

This EO, among other directives, identified the Department of Homeland Security (DHS), then in its nascent formation, as the federal agency authority to coordinate and work with other federal agencies involved in cybersecurity.

Homeland Security Policy Directive 7: Critical Infrastructure Identification, Prioritization, and Protection: President Bush issued HSPD-7 on December 17, 2003, explicitly replacing PDD-63, and clarifying the federal policy toward protecting critical infrastructure by directing that a national policy be "established for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks" using the definition of critical infrastructure defined by U.S. Patriot Act. Key resources are defined by the Homeland Security Act of 2002 as "Publicly or privately controlled resources essential to the minimal operations of the economy and government."

[2] President's Critical Infrastructure Protection Board. https://www.federalregister.gov/agencies/president-s-critical-infrastructure-protection-board

The strategy established 16 specific critical infrastructure sectors and designated a lead federal sector specific agency (SSA) for each. The Department of Energy is the SSA for the O&G industry, but not other energy industries such as nuclear, chemical, or electric power.

The 2006 National Infrastructure Protection Plan (NIPP) outlines the public-private partnership to "deter threats, mitigate vulnerabilities, and minimize consequences" and called for creating more sector-specific plans. The NIPP was replaced in 2009 (after President Obama's election) and emphasized the importance of resiliency and protection.

Presidential Directive 21: President Barack Obama expanded the power of DHS in Homeland Security Presidential Directive 21 (PPD-21) released on February 12, 2013. PPD-21 and the accompanying Executive Order 13636 established DHS as the government agency responsible for coordinating protection, prevention, mitigation, and recovery. In addition, PPD-21 directed the federal government Sector-Specific Agencies (SSAs) for day-to-day engagement with each of the 16 sectors[3]. The SSAs establish the required policies with industry and coordinate their regulation with DHS. The O&G gas industry is assigned to the Department of Energy for its SSA.

EO 13636: The order identified critical infrastructure as both "physical and cyber", introduced new information sharing programs, and directed the development of the NIST Cybersecurity Framework and a concomitant "voluntary" program encouraging industry to adopt the NIST Cybersecurity Framework.

PPD-21 and EO 13636 resulted from a GAO report that listed "Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructure" as one of 30 areas of risk identified that required attention by Congress and the Executive Branch in the GAO report, "High Risk Series, An update".

Executive Order 13800: On May 11, 2017, President Trump issued Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats to its digital and physical security.

1.3 European Union (E.U.)

The E.U. established the ***European Network and Information Security Agency*** (ENISA) in 2004 to coordinate cybersecurity between the 28 member states and their Computer Emergency Response Teams (CERTs), and provide training and support in cybersecurity (including offensive capabilities with the European Defense Agency). In addition, the E.U. established within Europol its ***European Cybercrime Centre*** (EC3), also in 2004, for sharing cyber crime information between law enforcement agencies.

The main policy in the E.U. is the ***European Cyber Security Strategy*** (2003) that established the goals of (1) achieving cyber resilience, (2) reducing cyber crime, (3) developing cyber defense policy and capabilities, (4) developing the industrial and technological resources for cybersecurity, and (5) establishing a coherent international cyberspace and promoting E.U. values. An important aspect is

[3] The National Strategy to Secure Cyberspace. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

the European coordination effort, since the Strategy seeks that each member state (1) designates a sole national agency as coordination for cybersecurity policy and operations, (2) has a sole CERT that would act as the operational center in case of a major cyber incident, and (3) ratifies the 2002 Budapest Convention as baseline for combating cybercrime. The Strategy is complemented by several legislations and policies, amongst which the most important is the ***Network and Information Security Directive*** (2014) that aims at operationalizing the goals of the Strategy by establishing minimum cybersecurity standards.

1.4 The United Kingdom (UK)

In 2012, the UK Government launched its 10 Steps to Cyber Security and subsequently "Small Businesses: What you need to know about cyber security" guidance to encourage organizations to consider whether they were managing their cyber risks. The UK Government emphasized the need for Company Boards and senior executives to take ownership of these risks and to enshrine them within their overall corporate risk management regime. The initiative was later revised into what is known as the Cyber Essential Scheme, which focuses on basic cyber hygiene. The Cyber Essential Scheme was developed by the UK Government in collaboration with the Information Assurance for Small & Medium Enterprises (IASME), the Information Security Forum (ISF), and the British Standards Institute (BSI).

The Cyber Essential scheme provides a clear statement of the basic controls all organizations should implement to mitigate the risk from common internet based threats and through the Assurance Framework it offers a mechanism for organizations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

2 OVERVIEW OF DRILLING CYBERSECURITY STANDARDS

There is no specific “Cybersecurity Standard for Drilling Control Systems” per se, although there are standards both for ICS and SCADA systems. Other standards, although generic in nature or developed for IT Cybersecurity, are also applicable.

Achieving an effective Cybersecurity strategy for O&G Drilling requires a contextualizing and tailoring effort. There are also several relevant Standards applicable to the context of O&G Drilling Cybersecurity that could be also taken into account as complementary information. This context includes areas such as Health, Safety, and Environment (HSE) and security in drilling (e.g., IADC Case Guidelines and API Standards), IT governance (e.g., ISACA Standards), and Business Continuity (ISO 22300-Series).

2.1 Cybersecurity Standards

The main standards in Cybersecurity are the ISO/IEC 27000-Series on Information Security Management Systems - common in Europe and Oceania - and the NIST SP-800 series on Computer Security - required in the United States. Both series have considerable overlap and are complementary, non-competing, standards. Each incorporates new standards through documents or annexes regarding OT Cybersecurity. In addition, ISA /IEC 62443 (formerly ISA/ANSI 99) is a relevant series of Standards for OT Cybersecurity.

These three families of standards (i.e., ISO, NIST, and ISA) combine to form the pillars of a sound Cybersecurity strategy. Eventually, these standards will likely converge and be more compatible. New NIST developments and revisions continue to align with ISO standards (i.e. aligning NIST SP-800 series with the ISO 27000-Series), and with ISA (e.g., NIST Cybersecurity Framework). ISA 62443 is aligned with both ISO and NIST standards, and other standard bodies at international level (IEC, International Electrotechnical Commission) and US level (ANSI, American National Standards Institute).

2.2 NIST Cybersecurity Framework

The NIST Framework for Improving Critical Infrastructure (2014), commonly known as the NIST Cybersecurity Framework, is a voluntary framework that comes from the requirement of the US Federal Government (EO 13636) for developing a risk-based framework to help organizations protect the critical infrastructures of the United States. The NIST Cybersecurity Framework guides operators of critical infrastructure and services in managing and improving cybersecurity risks, as part of the entire organization risk management processes. It does not provide new recommendations or practices, but it integrates, and refers to, best practices from other recognized standards. This integrative approach includes practices from governance to technical levels, and are tailored for IT and OT protection.

The framework has three sections:

- **Framework Core**. Cybersecurity practices with reference to the main standards that provide further information. These practices are grouped in five fundamental functions:
    - **Identify**. Understanding the business context, assets, resources and risk of the systems.
    - **Protect**. Best practices and measures to secure the systems against cyber threats.

    - **Detect**. Best practices and measures to detect cybersecurity events.
    - **Respond**. Best practices and measures to respond to cybersecurity incidents.
    - **Recover**. Best practices and measures to recover from cybersecurity incidents.
- **Framework Implementation Tiers**. Management and organizational guidance on how to improve the maturity of the cybersecurity practice of the organization. The tiers represent maturity levels from ad-hoc cybersecurity practices (partial tier) to a fully integrated and adaptive cybersecurity process (adaptive tier).
- **Framework Profile**. Assessment of the organization cybersecurity profile to help the organization to assess gaps in current cybersecurity practice and to optimize the overall cybersecurity strategy.

Although it is voluntary, an organization following the NIST Cybersecurity Framework will show a proactive adherence to regulatory compliance and risk management practices. Also, the framework common language provides a way to improve the coordination and collaboration with other organization functions and external parties.

2.3 ISO/IEC 27000-Series Core Standards (27000-27005)

ISO/IEC 27000-Series are a common and agreed international framework, employed by national standardization bodies, to develop more detailed and tailored Standards applicable in their respective countries. ISO 27000-Series cover dozens of standards, of which the most important are described below.

The initial standards of the ISO/IEC 27000-Series represent the core of the series and are commonly employed across industries. These Standards provide the framework to establish and implement the ***Information Security Management System*** defined by the series, including requirements, implementation, measurement, and risk management.

ISO/IEC 27000-Series Core Standards are the following:

- ISO/IEC 27000:2014 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary
- ISO/IEC 27001:2013 IT-ST – ISMS – Requirements
- ISO/IEC 27002:2013 IT-ST – Code of Practice for Information Security Controls
- ISO/IEC 27003:2010 IT-ST – ISMS Implementation Guidance
- ISO/IEC 27004:2009 IT-ST – ISMS - Measurement
- ISO/IEC 27005:2011 IT-ST – Information Security Risk Management

2.4 NIST Risk Management Framework Standards

NIST also has a myriad of standards, but it has defined a risk management framework (RMF) that comprises the most relevant NIST SP-800 series standards as well as FIPS (Federal Information Processing Standards) 199 and 200. The RMF establish a cybersecurity and risk management process comprised of a number of steps:

1. Categorize information systems (FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems, NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories)

2. Select security controls (FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems, NIST SP 800-53 Rev.4 Recommended Security Controls for Federal Information Systems and Organizations)
3. Implement security controls (NIST SP 800-160 Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems)
4. Assess security controls (NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations)
5. Authorize information system (NIST SP 800-37 Guide for Applying Risk Management Framework to Federal Information Systems)
6. Monitor security controls (NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations)

2.5 ISA Core Standards

ISA/IEC 62443 is a series of Standards (recently renamed from ISA 99) focusing on *Security for Industrial Automation and Control Systems*. There are currently 13 documents identified in the series:

- ISA-62443-1-1/IEC 62443-1-1 (TS): Security for Industrial Automation and Control Systems - Part 1-1: Models and Concepts
- ISA-TR62443-1-2/IEC 62443-1-2 (TR): Security for Industrial Automation and Control Systems - Part 1-2: Master Glossary of Terms and Abbreviations
- ISA-62443-1-3/IEC 62443-1-3: Security for Industrial Automation and Control Systems - Part 1-3: System Security Compliance Metrics
- ISA-TR62443-1-4/IEC 62443-1-4 (TR): Security for Industrial Automation and Control Systems - Part 1-4: Security Life Cycle and Use Cases
- ISA-62443-2-1/IEC 62443-2-1: Security for Industrial Automation and Control Systems - Part 2-1: Requirements for an IACS Security Management System
- ISA-TR62443-2-2/IEC 62443-2-2 (TR): Security for Industrial Automation and Control Systems - Part 2-2: Implementation Guidance for an IACS Security Management System
- ISA-TR62443-2-3/IEC 62443-2-3 (TR): Security for Industrial Automation and Control Systems - Part 2-3: Patch Management in the IACS Environment
- ISA-62443-2-4/IEC 62443-2-4: Security for Industrial Automation and Control Systems - Part 2-4: Requirements for IACS Solution Suppliers
- ISA-TR62443-3-1/IEC 62443-3-1 (TR): Security for Industrial Automation and Control Systems - Part 3-1: Security Technologies for IACS
- ISA 62443-3-2/IEC 62443-3-2: Security for Industrial Automation and Control Systems - Part 3-2: Security Risk Assessment and System Design
- ISA-62443-3-3/IEC 62443-3-3: Security for Industrial Automation and Control Systems - Part 3-3: System Security Requirements and Security Levels
- ISA-62443-4-1/IEC 62443-4-1: Security for Industrial Automation and Control Systems - Part 4-1: Product Development Requirements
- ISA-62443-4-2/IEC 62443-4-2: Security for Industrial Automation and Control Systems - Part 4-2: Technical Security Requirements for IACS Components

2.6 Norwegian Continental Shelf

OLF (Oljeindustriens landsforening) or the Norwegian Oil and Gas Association have published two cybersecurity guidelines for process control systems and networks: OLF 104 - Recommended Guideline for Information Security Baseline Requirements for Process Control, Safety and Support Systems, and OLF 110 - Recommended Guidelines for Implementation of Information Security in Process Control, Safety and Support Systems during the Engineering, Procurement and Commissioning Phases. **OLF Recommended Guideline 104 (2009)** focuses on process control, safety, and support networks, and defines mandatory baseline cybersecurity requirements.

3 CYBERSECURITY SOLUTION REQUIREMENTS FOR O&G DRILLING ASSETS

3.1 Introduction

The NIST Cybersecurity Framework defines five core cybersecurity functions:

Function	Definition
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Table 1: NIST Cybersecurity Framework Categories and Functions

3.2 Identify

The following requirements are derived from the IADC Guideline for Cybersecurity Risk Assessment and Management of Drilling Assets:

I1. Cyber assess and manage all drilling assets periodically according to standards and industry best practices (e.g. the IADC Guideline).

The following requirements are derived from the DHS Industrial Control System (ICS) Computer Emergency Response Team (CERT) recommended practice:

I2. Establish and maintain an asset inventory for all ICS (hardware, firmware, software, applications, network diagrams, protocols, etc.).

I3. Establish and maintain an overview of connections to and interconnection within the control systems of the drilling asset.

I4. Identify all remote connections and how these connections interact with ICS.

3.3 Protect

The following requirements are derived from ISA/IEC 62443: Security for Industrial Automation and Control Systems (IACS):

P1. Implement cybersecurity functions to segregate IT systems from ICS.

P2. Implement cybersecurity functions to segregate various ICS.

P3. Implement cybersecurity functions to control remote connections and how these connections interact with ICS.

P4. Implement cybersecurity functions to control access to servers, ICS equipment, networking equipment, security appliances, and mobile devices where applicable.

The following requirements are derived from the DHS Industrial Control System (ICS) Computer Emergency Response Team (CERT) recommended practice:

P5. Remove all features, functions, external connections, software, hardware, etc. that is not in use or necessary for the successful functioning of the ICS.

P6. Develop and maintain cybersecurity awareness education so that the organization's personnel and partners are adequately trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

3.4 Detect

The following requirements are derived from the NIST Cybersecurity Framework:

D1. Deploy capabilities to ensure that anomalous activity is detected in a timely manner and that the potential impact of events is understood.

D2. Deploy capabilities to ensure that the ICS are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

D3. Deploy capabilities to verify that detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

3.5 Respond

The following requirements are derived from the NIST Cybersecurity Framework:

RD1. Develop, implement and maintain Cybersecurity event and incident response plans according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure). The plans should cover roles and responsibilities and address both IT and OT systems important for the delivery of the function.

RD2. Deploy capabilities to verify that cybersecurity events and incident response is performed according to the appropriate incident response plans.

RD3. Develop, implement and maintain appropriate training for cybersecurity event and incident response teams.

3.6 Recover

The following requirements are derived from the NIST Cybersecurity Framework:

RR1. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. This requirement refers to incident recovery plans and procedures.

RR2. Identify the activities necessary to sustain minimum operations of the function.
RR3. Develop, implement and maintain continuity plans to sustain and restore operation of the function.
RR4. Develop, implement and maintain recovery plans describing the sequence of activities necessary to return the function to normal operation.

4 REFERENCES

- National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.0. February 12, 2014.
- International Association of Drilling Contractors (IADC). *Guidelines for Risk Management and Assessment Standards and Methods to use for Assessing Cybersecurity Risks of Drilling Assets*. March 2016.
- DHS Industrial Control System (ICS) Computer Emergency Response Team (CERT). *Recommended Practice*. September 2016.International Society for Automation. *ISA 62443 – Security for Industrial Automation and Control Systems.*

ANNEX 1. DOCUMENT HISTORY

Document History		
Version	**Date**	**Description**
0.1	Nov 14, 2016	Initial requirement set provided as input into IADC ART Cybersecurity Subcommittee Meeting Nov 15, 2016.
0.2	Nov 16, 2016	Update of initial requirement set based on IADC ART Cybersecurity Subcommittee Meeting feedback.
0.5	March 09, 2017	Updated requirements based on results of JM with USCG, NIST NCCoE, MITRE on MODU Profile.
0.6	May 09, 2017	Refined some of the requirements based on review comments. Also, shortened the section on US regulatory landscape to align with the portion on EU.
0.7	May 10, 2017	Corrected typos and improved the language.
0.8	May 11, 2017	Updated structure of the document and some of the requirements based on the input from the May 11 subcommittee meeting.
1.0	Aug 2, 2017	Updated with input from the July 13 subcommittee meeting.