CableLabs
Security

Zero Trust and Infrastructure Security Best Common Practices

CL-GL-ØTIS-BCP-V01-240924

RELEASED

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, infringement, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CL-GL-ØTIS-BCP-V01-240924			
Document Title:	Zero Trust and Infrastructure Security Best Common Practices			
Revision History:	Released – 9/24/2024			
Date:	September 24, 2024			
Status:	~~Work in Progress~~	~~Draft~~	**Released**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ NDA Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document that is considered largely complete, but lacking review by members and vendors. Drafts are susceptible to substantial change during the review process.
Released	A generally public document that has undergone rigorous member and technology supplier review, cross-vendor interoperability, and is suitable for certification/qualification testing if applicable.
Closed	A static document, reviewed, tested, validated, and closed to further changes.

Trademarks

Contents

1 SCOPE 6
1.1 Introduction and Overview 6
1.2 Purpose of Document 7
1.2.1 Zero Trust 7
1.2.2 Secure Automation 7
1.2.3 Security Monitoring 8
1.2.4 Consistent Security Control 8
2 REFERENCES 9
2.1 Informative References 9
3 TERMS AND DEFINITIONS 12
4 ABBREVIATIONS 13
5 REQUIREMENTS COMPLIANCE 15
5.1 Compliance Classification 15
5.1.1 Compliance through Disclosure and Documentation 15
5.1.2 Compliance through Attestation by Vendor 15
5.1.3 Compliance through Automated Testing/Tools 15
5.1.4 Compliance through Manual Verification 15
6 TECHNICAL REQUIREMENTS 16
6.1 Credential and Secret Storage (KEY)—General Requirements 16
6.1.1 KEY Requirements Clarifications 16
6.2 Identity and Access Management (IAM)—General Requirements 17
6.2.1 IAM Requirements Clarifications 17
6.2.2 IAM Operators Common Practices 19
6.3 Security Associations (SA) 19
6.3.1 Security Associations General (SA-GEN) Requirements 19
6.3.2 SA-GEN Requirements Clarifications 19
6.3.3 Element Authentication (SA-EAN) Requirements 20
6.3.4 SA-EAN Requirements Clarifications 20
6.3.5 Element Authorization (SA-EAZ) Requirements 21
6.3.6 SA-EAZ Requirements Clarifications 21
6.3.7 SA-EAZ Operators Common Practices 21
6.3.8 User Authentication (SA-UAN) Requirements 22
6.3.9 SA-UAN Requirements Clarifications 22
6.3.10 User Authorization (SA-UAZ) Requirements 22
6.3.11 SA-UAZ Requirements Clarifications 22
6.4 Asset Inventory and Management (AIM) 23
6.4.1 Asset Management and Inventory General (AIM-GEN) Requirements 23
6.4.2 AIM-GEN Requirements Clarifications 24
6.4.3 Software Asset Management (AIM-SW) Requirements 25
6.4.4 AIM-SW Requirements Clarifications 25
6.4.5 Hardware Asset Management (AIM-HW) Requirements 27
6.4.6 AIM-HW Requirements Clarifications 27
6.4.7 Data Asset Management (AIM-DT) Requirements 27
6.4.8 AIM-DT Requirements Clarifications 28
6.4.9 Account Asset Management (AIM-AC) Requirements 28
6.4.10 AIM-AC Requirements Clarifications 28
6.5 Measurement and Attestation (MA) 29
6.5.1 Measurement and Attestation General (MA-GEN) Requirements 29
6.5.2 MA-GEN Requirements Clarifications 29

6.5.3 Boot Security General (MA-BT) Requirements 29
6.5.4 MA-BT Requirements Clarifications 29
6.5.5 Secure Boot (MA-SB) Requirements 30
6.5.6 MA-SB Requirements Clarifications 30
6.5.7 Measured Boot (MA-MB) Requirement 31
6.5.8 MA-MB Requirement Clarification 31
6.5.9 Integrity of Time (MA-TS) Requirement 31
6.5.10 MA-TS Requirement Clarification 31
6.5.11 Integrity of Configuration and State (MA-ICS) Requirements 31
6.5.12 MA-ICS Requirements Clarifications 32
6.6 Security Information and Event Management (SIEM)—General Requirements 32
6.6.1 SIEM Requirements Clarifications 32
6.7 Reliability and Availability (RA) 33
6.7.1 Reliability and Availability General (RA-GEN) Requirements 33
6.7.2 RA-GEN Requirements Clarifications 33
6.7.3 Incident Response (RA-IR) Requirements 33
6.7.4 RA-IR Requirements Clarifications 34
6.8 Configuration and Change Management (CCM)—General Requirements 34
6.8.1 CCM Requirements Clarifications 34

APPENDIX I ACKNOWLEDGEMENTS 36

Tables

Table 1 - Credential and Secret Storage General Requirements (KEY) 16
Table 2 - Identity and Access Management General Requirements (IAM) 17
Table 3 - Security Associations General Requirements (SA-GEN) 19
Table 4 - Element Authentication Requirements (SA-EAN) 20
Table 5 - Element Authorization Requirements (SA-EAZ) 21
Table 6 - User Authentication Requirements (SA-UAN) 22
Table 7 - User Authorization Requirements (SA-UAZ) 22
Table 8 - Asset Management and Inventory General Requirements (AIM-GEN) 23
Table 9 - Software Asset Management Requirements (AIM-SW) 25
Table 10 - Hardware Asset Management Requirements (AIM-HW) 27
Table 11 - Data Asset Management Requirements (AIM-DT) 27
Table 12 - Account Asset Management Requirements (AIM-AC) 28
Table 13 - Measurement and Attestation General Requirements (MA-GEN) 29
Table 14 - Boot Security General Requirements (MA-BT) 29
Table 15 - Secure Boot Requirements (MA-SB) 30
Table 16 - Measured Boot Requirement (MA-MB) 31
Table 17 - Integrity of Time Requirement (MA-TS) 31
Table 18 - Integrity of Configuration and State Requirements (MA-ICS) 31
Table 19 - Security Information and Event Management General Requirements (SIEM) 32
Table 20 - Reliability and Availability General Requirements (RA-GEN) 33
Table 21 - Incident Response Requirements (RA-IR) 33
Table 22 - Configuration and Change Requirements (CCM) 34

Figures

Figure 1 - Architecture Scope of Zero Trust Infrastructure Security (ØTIS) 6

1 SCOPE

1.1 Introduction and Overview

This Zero Trust and Infrastructure Security (ØTIS) document specifies the best common practices that will serve as an industry guideline for infrastructure elements (i.e., manageable physical and/or virtualized components within operator's network) used when implementing zero trust concepts (Figure 1). This document provides a security framework for infrastructure elements and is developed with operators' contributions.

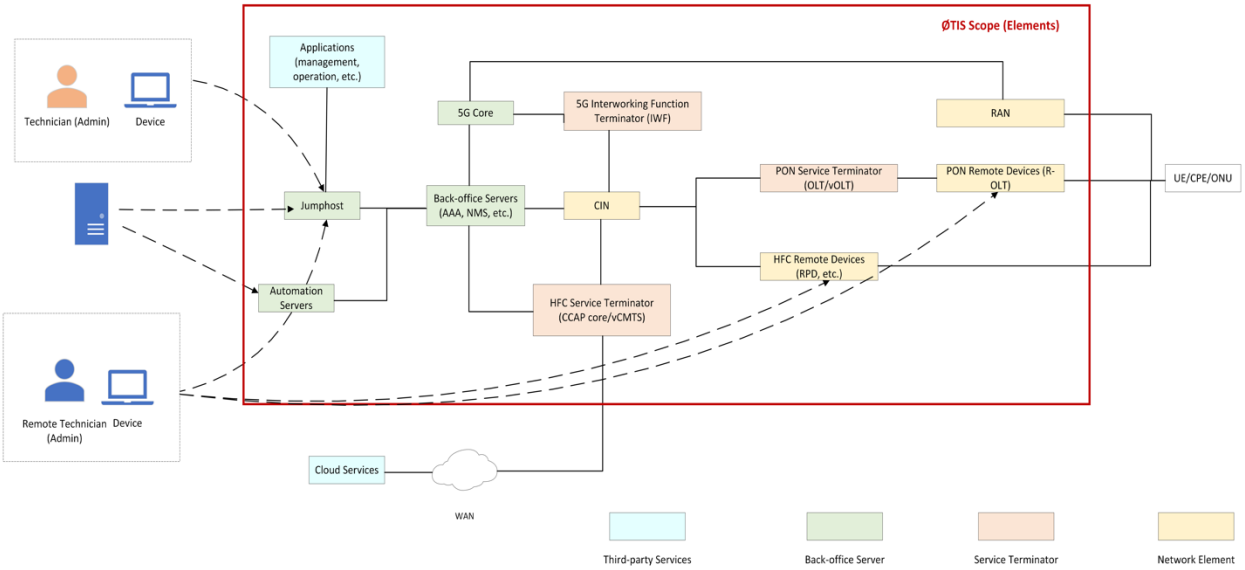

Figure 1 - Architecture Scope of Zero Trust Infrastructure Security (ØTIS)

This document uses the term "element" for any managed physical or virtualized components within an operator's network, including all the transport, compute, and storage components necessary to delivery broadband services. An element will always be an endpoint on the management plane and may be a transport element (via) on the user data plane. Some examples of elements are listed below:

- service terminators such as OLT, CMTS, CCAP, CCAP Core, 5G Interworking Function Terminator (IWF);
- remote devices such as RPD, RMD, and R-OLT;
- Converged Interconnect Network (CIN) components such as switches and routers between core and remote devices;
- HFC security elements such as smart amplifier, managed fiber node, and managed power supply; and
- back-office servers such as network management systems (NMS), provisioning servers, and AAA servers.

This document uses the term "interface" for any physical, logical, network, or virtual communication port that is implemented on the device. Interfaces include but are not limited to the following:

- local communications ports (serial, USB);
- network interfaces like ethernet, Wi-Fi, and Bluetooth;
- IP listen ports/sockets;
- virtualized interfaces; and
- interfaces meant for operator management of the device.

1.2 Purpose of Document

The purpose of this document is to provide a common set of requirements and best practices for MSOs and vendors to support zero trust concepts, secure automation, security monitoring, and consistent security control. Note that each MSO may have additional or different requirements from those specified in this document. By capturing many of the common and core requirements shared among cable operators, this document will be informative to vendors and provide a common language to facilitate the sharing of best practices.

The requirements and best practices cover the following areas:

- credential protection and secure storage,
- identity security and data protection,
- asset and inventory management,
- supply chain risk management,
- secure automation,
- security monitoring and incident responses,
- boot security,
- policy-based access management, and
- consistent security control.

1.2.1 Zero Trust

Zero trust refers to an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to a focus on users, assets, and resources ([NIST 800-207]). The core idea of zero trust is the assumption that there is no inherited or default trust in the infrastructure network and the trust and permission should be guaranteed only after certain verification processes with consistent policy-based security controls ("never trust, always verify"). In this document, supporting zero trust for infrastructure security means providing an end-to-end approach for infrastructure elements to secure data and control planes. The goal of supporting zero trust in this document is to increase resilience against attacks from within the broadband infrastructure which may extend beyond the enterprise of the operator in a DevSecOps and SCRM (supply chain risk management) context.

Some examples of zero trust common practices include

- implementing security associations for all link and network connections,
- using multi-factor authentication (MFA) for non-machine entities' access and logging all access, and
- implementing dynamic policy-based access controls for users and elements regardless of their network locations.

Requirements in this document should align with the seven tenets of zero trust as specified in [NIST 800-207], the zero trust pillars of CISA Zero Trust Maturity Model 2.0 ([CISA ZTMM 2.0]), and the NIST Cybersecurity Framework 2.0 ([NIST CSF 2.0]).

1.2.2 Secure Automation

In this document, secure automation means to apply secure and reliable software practices to IT systems to reduce human involvement and improve network and system optimization capabilities. The goal of secure automation is to facilitate connectivity to allow automated deployment, operation, and maintenance of broadband service delivery with security and privacy and reliability natively built in and automated as much as possible, without adversely reducing options.

Some examples of secure automation include

- using consistent credentialling to enable automatic establishment of security associations between machines, over links, and across interfaces;

- defining and requiring probation time (soak time) for automated tools and operators before implementing in real environment; and
- implementing automated tools for network provisioning and credential management.

1.2.3 Security Monitoring

In this document, security monitoring refers to maintaining an ongoing awareness of broadband infrastructure security, vulnerabilities, and threats to support the security goals of the service delivery. The goal of security monitoring is to ensure continued effectiveness of security controls and verify compliance with established broadband infrastructure security requirements.

Some examples of security monitoring include

- detecting and collecting security events information from operator's network components and integrating it into operational security information and events management systems,
- continuously monitoring security posture and configuration and ensuring compliance with designed security policies, and
- reviewing technology changes and advancements for impact to security policies and updating those policies as needed.

1.2.4 Consistent Security Control

In this document, consistent security control requires operators to have a consistent process to describe and assert end-to-end security controls ubiquitously across the broadband service delivery network. The goal of consistent security control is to ensure all elements and processes are equivalently secured using methods that are well understood by supporting staff. Automation helps to assure consistent security control, but automation also requires additional controls.

Some examples of consistent security control include

- reviewing current security controls and periodically updating controls to align with the most current security standards and policies,
- providing configuration templates and security hardening guidelines for managed infrastructure elements with version controls and roll back processes, and
- providing regular training to raise security awareness and improve the ability to respond to cyber incidents and attacks.

2 REFERENCES

2.1 Informative References

The following references include documents/links to standards in different regions including EU and North America) in order to align recommendations within this document with these references.

[2020 CWE 25] 2020 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses, https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

[BCMO] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, M. Dworkin, December 2001, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[BCMO-CCM] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, M. Dworkin, May 2004, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[BCMO-GCM] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, M. Dworkin, November 2007, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[BCMO-Key Wrap] NIST Special Publication 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, M. Dworkin, December 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38f.pdf

[BCMO-XTS-AES] NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, M. Dworkin, January 2010, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

[CA SB-327] California SB-327 Information Privacy: Connected Devices, September 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

[CISA HBOM] CISA, Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management, September 2023, https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management

[CISA VEX] CISA, When to Issue VEX Information, November 2023, https://www.cisa.gov/resources-tools/resources/when-issue-vex-information

[CISA ZTMM 2.0] CISA Zero Trust Maturity Model, Version 2.0, April 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[CVSS] Common Vulnerability Scoring System v3.1: Specification Document, https://www.first.org/cvss/v3.1/specification-document

[CycloneDX] OWASP Foundation, CycloneDX, https://cyclonedx.org/

[ESTI EN 303 645] ETSI EN 303 645, V2.1.1, CYBER—Cyber Security for Consumer Internet of Things: Baseline Requirements, June 2020, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[FIPS 140-3] NIST FIPS 140-3, Security Requirements for Cryptographic Modules, March 2019, https://csrc.nist.gov/publications/detail/fips/140/3/final

[FIPS 180-4] NIST FIPS 180-4, Secure Hash Standard (SHS), August 2015, https://csrc.nist.gov/pubs/fips/180-4/upd1/final

[FIPS 186-5] NIST FIPS 186-5, Digital Signature Standard (DSS), February 2023, https://csrc.nist.gov/pubs/fips/186-5/final

[IEEE 1588-2019] IEEE 1588-2019, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (Precision Time Protocol), June 2020, https://standards.ieee.org/standard/1588-2019.html

[NIST 800-56A] NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis, April 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

[NIST 800-56B] NIST Special Publication 800-56-B Revision 2, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, E. Barker, L. Chen, A. Roginsky, A. Vassilev, R. Davis, S. Simon, March 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

[NIST 800-56C] NIST Special Publication 800-56C Revision 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, E. Barker, L. Chen, R. Davis, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

[NIST 800-63-3] NIST Special Publication 800-63 Revision 3, Digital Identity Guidelines, P. Grassi, M. Garcia, J. Fenton, June 2017, https://pages.nist.gov/800-63-3/sp800-63-3.html

[NIST 800-63B] NIST Special Publication 800-63B, Digital Identity Guidelines—Authentication and Lifecycle Management, P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, June 2017, https://pages.nist.gov/800-63-3/sp800-63b.html

[NIST 800-63C] NIST Special Publication 800-63C, Digital Identity Guidelines—Federation and Assertions, P. Grassi, J. Richer, S. Squire, J. Fenton, E. Nadeau, June 2017, https://pages.nist.gov/800-63-3/sp800-63c.html

[NIST 800-92] NIST Special Publication 800-92, Guide to Computer Security Log Management, K. Kent, M. Souppaya, September 2006, https://csrc.nist.gov/pubs/sp/800/92/final

[NIST 800-133] NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, E. Barker, A. Roginsky, R. Davis, June 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

[NIST 800-154] NIST Special Publication 800-154, Guide to Data-Centric System Threat Modeling, M. Souppaya, K. Scarfone, March 2016, https://csrc.nist.gov/pubs/sp/800/154/ipd

[NIST 800-162] NIST Special Publication 800-163, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, V. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, January 2014, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[NIST 800-207] NIST Special Publication 800-207, Zero Trust Architecture, S. Rose, O. Borchert, S. Mitchell, S. Connelly, August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[NIST 7622] NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, J. Boyens, C. Paulsen, N. Bartol, R. Moorthy, S. Shankles, October 2012, https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

[NIST 8259A] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, M. Fagan, K. Megas, K. Scarfone, M. Smith, May 2020, https://doi.org/10.6028/NIST.IR.8259A

[NIST 8496 ipd] NIST 8496 ipd, Data Classification Concepts and Considerations for Improving Data Collection, W. Newhouse, M. Souppaya, J. Kent, K. Sandlin, K. Scarfone, November 2023, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8496.ipd.pdf

[NIST CSF 2.0] The NIST Cybersecurity Framework (CSF) 2.0, February 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[NTIA SBOM] National Telecommunications and Information Administration, Software Bill of Materials, https://www.ntia.gov/page/software-bill-materials

[OWASP 10] OWASP, Top 10 Web Application Security Risks—Injection, 2021, https://owasp.org/Top10/A03_2021-Injection/

[RFC 3411] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, D. Harrington, R. Presuhn, B. Wijnen, December 2002, https://www.rfc-editor.org/rfc/rfc3411

[RFC 4250] IETF RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers, S. Lehtinen, C. Lonvick, January 2006, https://datatracker.ietf.org/doc/html/rfc4250

[RFC 4251] IETF RFC 4251, The Secure Shell (SSH) Protocol Architecture, T. Ylonen, C. Lonvick, January 2006, https://datatracker.ietf.org/doc/html/rfc4251

[RFC 4252] IETF RFC 4252, The Secure Shell (SSH) Authentication Protocol, T. Ylonen, C. Lonvick, January 2006, https://datatracker.ietf.org/doc/html/rfc4252

[RFC 4253] IETF RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, T. Ylonen, C. Lonvick, January 2006, https://datatracker.ietf.org/doc/html/rfc4253

[RFC 4254] IETF RFC 4254, The Secure Shell (SSH) Connection Protocol, T. Ylonen, C. Lonvick, January 2006, https://datatracker.ietf.org/doc/html/rfc4254

[RFC 4492] IETF RFC 4492, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller, May 2006, https://datatracker.ietf.org/doc/html/rfc4492

[RFC 5116] IETF RFC 5116, An Interface and Algorithms for Authenticated Encryption, D. McGrew, January 2008, https://datatracker.ietf.org/doc/html/rfc5116

[RFC 5246] IETF RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, T. Dierks, E. Rescorla, August 2008, https://datatracker.ietf.org/doc/html/rfc5246

[RFC 5424] IETF RFC 5424, The Syslog Protocol, R. Gerhards, March 2009, https://datatracker.ietf.org/doc/html/rfc5424

[RFC 5425] IETF RFC 5425, Transport Layer Security (TLS) Transport Mapping for Syslog, F. Miao, Y. Ma, J. Salowey, March 2009, https://datatracker.ietf.org/doc/html/rfc5425

[RFC 5905] Network Time Protocol Version 4: Protocol and Algorithms Specification, D. Mills, J. Martin, J. Burbank, W. Kasch, June 2010, https://tools.ietf.org/html/rfc5905

[RFC 8446] IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, E. Rescorla, August 2018, https://tools.ietf.org/html/rfc8446

[RFC 8633] IETF RFC 8633, Network Time Protocol Best Current Practices, D. Reilly, H. Stenn, D. Sibold, July 2019, https://tools.ietf.org/html/rfc8633

[RFC 8915] IETF RFC 8915, Network Time Security for the Network Time Protocol, D. Franke, D. Sibold, K. Teichel, M. Dansarie, R. Sundblad, September 2020, https://tools.ietf.org/html/rfc8915

[RFC 8996] IETF RFC 8996, Deprecating TLS 1.0 and TLS 1.1, K. Moriarty, S. Farrell, March 2021, https://tools.ietf.org/html/rfc8996

[RFC 9142] IETF RFC 9142, Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH), M. Baushke, January 2022, https://datatracker.ietf.org/doc/html/rfc9142

[SPDX] ISO/IEC 5962:2021, Information Technology—SPDX® Specification V2.2.1, August 2021, https://www.iso.org/standard/81870.html

[SWID] NIST, Software Identification (SWID) Tagging, https://csrc.nist.gov/projects/Software-Identification-SWID

[WFA Security] Wi-Fi Certified WPA3 Specification, https://www.wi-fi.org/discover-wi-fi/security

3 TERMS AND DEFINITIONS

asset	An item of value to operators that can be either tangible or intangible. Examples of assets include but are not limited to management accounts, cryptographic keys or other primitives (particularly necessary for assessing cryptographic reediness for PQC transition), credentials or certificates, configuration files, licenses, or any other aspect of the element necessary for its intended function or to configure its operation.
attestation	The process of verifying a set of fresh measurements and indicating whether the status or behavior of an element complies with preset conditions or policies.
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
cable modem (CM)	A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.
Cable Modem Termination System (CMTS)	A device located at the cable television system headend or distribution hub that provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.
credential	An object or data structure that authoritatively binds an identity, via an identifier or identifiers, and (optionally) additional attributes, to at least one authenticator possessed and controlled by operators. This definition includes logins and associated passwords.
element	Any managed physical or virtualized component located northbound of the customer network and southbound of the operator's core network (and including all the transport, compute, and storage components necessary to delivery broadband services). It will always be an endpoint on the management plane and may be a transport element (via) on the user data plane.
firmware	Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM) such that the programs and data cannot be dynamically written or modified during execution of the programs.
hardware components	Tangible physical components used by infrastructure elements such as TPMs, memory sticks, bear mental servers, switches that enable operators to manage and/or monitor their networks, elements, and services.
hardware root of trust (HwRoT)	An inherently trusted combination of hardware and firmware that maintains the integrity of information.
identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of the management domain, is sufficient to distinguish that entity from any other entity.
integrity protection	A physical or cryptographic means of providing assurance that information has not been altered in an unauthorized manner since it was created, transmitted, or stored.
managed element	An element is said to be "managed" if an organization has administrative control of the element and can apply security policy to it; otherwise, the element is considered unmanaged.
measurement	The active process of promptly collecting and recording quantitative values that reflect the behavior or status of an element. The measurement process usually uses formulas to calculate values stored in metrics (i.e., the measurement results are derived from certain metrics). A timely measurement that is signed can be used for attestation of an element to demonstrate that it complies with the preset conditions or policies.
PNM server	One or more software application(s) for initiating PNM tests and queries involving network elements, acting as a server from the perspective of other PNM and OSS applications, but acting as a client for network elements and measurement devices providing PNM and OSS results.
sensitive data	Information whose loss, misuse, or unauthorized access or modification could adversely affect security.
SNMP agent	The term "agent" is used throughout this document to refer to (1) an SNMPv1/v2 agent or (2) an SNMPv3 entity [RFC 3411] that contains command responder and notification originator applications.
SNMP manager	The term "manager" is used throughout this document to refer to (1) an SNMPv1/v2 manager or (2) an SNMPv3 entity [RFC 3411] that contains command generator and/or notification receiver applications.
software components	Software assets such as libraries, firmware, or source code.
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
trust anchor	An authoritative entity for which trust is assumed and not derived. For example, the root certificate acts as the trust anchor from which the chain of trust is derived.

4 ABBREVIATIONS

ØTIS	Zero Trust Infrastructure Security
ABAC	Attribute-Based Access Control
AEAD	Authenticated Encryption with Additional Data
AES	Advanced Encryption Standard
AGF	Access Gateway Function
API	Application Programming Interface
BNG	Broadband Network Gateway
CBC	Cipher Block Chaining
CCAP	Converged Cable Access Platform
CIN	Converged Interconnect Network
CISA	Cybersecurity and Infrastructure Security Agency, U.D. Department of Homeland Security
CLI	Command Line Interface
CMTS	Cable Modem Termination System
CRL	Certificate Revocation List
DBMS	Database Management System
DNS	Domain Name System
DUT	Device Under Test
FSBL	First Stage Boot Loader
FTP	File Transfer Protocol
GCM	Galois/Counter Mode
HBOM	Hardware Bill of Materials
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
mDNS	Multicast Domain Name System
MFA	Multi-Factor Authentication
MSO	Multiple System Operator
NETCONF	Network Configuration Protocol
NMS	Network Management Systems
OCSP	Online Certificate Status Protocol
OLT	Optical Line Terminal
OSP	Outside Plant
OSS	Operations Support System
OTP	One-Time Password
OTP	One Time Programmable
PEP	Policy Enforcement Point
PFS	Perfect Forward Secrecy
PII	Personally Identifiable Information
PKI	Public Key Infrastructure

PNM	Proactive Network Maintenance
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
PROM	Programmable Read-Only Memory
R-OLT	Remote Optical Line Terminal
RESTCONF	Representational State Transfer Configuration Protocol
RMD	Remote MACPHY Device
ROM	Read-Only Memory
RPD	Remote PHY Device
RPMB	Replay Protection Memory Block
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIV	Synthetic Initialization Vector
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
SSH	Secure Shell Protocol
TEE	Trusted Execution Environment
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UI	User Interface
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VEX	Vulnerability Exploitability eXchange
WAN	Wide Area Network

5 REQUIREMENTS COMPLIANCE

The following requirement key words are used within this document.

- SHALL—This word means that the definition is as an absolute requirement of this document.
- SHALL NOT—This phrase means that the definition is an absolute prohibition of this document.
- SHOULD—This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

5.1 Compliance Classification

The requirements outlined in this document cover a wide range of criteria, and it is important that there is a mechanism in place by which the vendor can prove or demonstrate that their product complies with the requirements. Depending on the requirement, compliance checks are done by one of the following verification steps.

5.1.1 Compliance through Disclosure and Documentation

Certain requirements, such as disclosing all open-source components used and their versions, are met in the form of relevant documents and links to information about how the vendor incorporated a specific feature in their product.

5.1.2 Compliance through Attestation by Vendor

Requirements that are not easily testable (either manually or using tools) need to be attested by the vendor, and compliance is confirmed through a legal agreement or disclosure. The customer/client also has the right to test/assess for compliance and not require explicit permissions for it (e.g., pen testing, destructive testing).

5.1.3 Compliance through Automated Testing/Tools

Requirements that can be validated by the use of automated tooling will be tested by providing artifacts (e.g., binary firmware images, flash dumps, source code, or similar) into a tool for analysis. This will be done by the customer/client or their authorized consultants/vendor. Results will be analyzed to ensure accuracy.

5.1.4 Compliance through Manual Verification

Requirements that can be validated by manual analysis are to be tested by basic dynamic testing (e.g., network scans) or an in-depth hardware or firmware penetration test (as needed). This is done by the customer/client or their authorized consultants/vendor.

6 TECHNICAL REQUIREMENTS

The requirements are categorized in the following functional areas.

1. Credential and Secret Storage (KEY)
2. Identity and Access Management (IAM)
3. Security Associations (SA)
4. Asset Management and Inventory (AIM)
5. Measurement and Attestation (MA)
6. Security Information and Event Management (SIEM)
7. Reliability and Availability (RA)
8. Configuration and Change Management (CCM)

6.1 Credential and Secret Storage (KEY)—General Requirements

Table 1 - Credential and Secret Storage General Requirements (KEY)

REQ#	Description	Status/Comment
KEY-001	Any private keys or secret keys that are stored on the element SHALL be stored in tamper-resistant hardware-based secure storage or encrypted by a key-encryption key stored in tamper-resistant hardware-based secure storage.	
KEY-002	Any trust anchors that are stored on the element SHALL be integrity protected by a key-encryption key, an integrity key, or a hash value stored in tamper-resistant hardware-based secure storage.	
KEY-003	An element SHALL verify the integrity of trust stores before using any stored trust anchors.	
KEY-004	An element SHALL use a [FIPS 140-3]-compliant version of a cryptographic library for new protocol implementations.	
KEY-005	All symmetric keys used for secure boot SHOULD be device unique.	

6.1.1 KEY Requirements Clarifications

KEY-001

Key-encryption key should provide security strength of at least 128 bits. Tamper-resistant storage mechanisms are expected to be implementation specific.

KEY-002

Refer to KEY-001 for more details of key-encryption key and tamper-resistant storage mechanisms.

KEY-003

No further clarification

KEY-004

No further clarification

KEY-005

This requirement is for use cases in which the element uses symmetric keys that are used to decrypt or encrypt code blocks during the secure boot process; this is an optional feature for secure boot.

6.2 Identity and Access Management (IAM)—General Requirements

Table 2 - Identity and Access Management General Requirements (IAM)

REQ#	Description	Status/Comment
IAM-001	An element SHALL NOT enable by default a hard-coded or weak password.	
IAM-002	An element SHALL require that if a non-unique initial/default password is present, it be changed to a strong password upon initial setup.	
IAM-003	An element SHOULD require that any element-unique default password be changed upon initial setup.	
IAM-004	An element SHALL store any passwords in a salted and hashed form.	
IAM-005	An element SHALL NOT use global administrative passwords.	
IAM-006	An infrastructure element that uses administrative passwords for access SHALL use element-unique administrative passwords.	
IAM-007	An element SHALL NOT allow remote access to the user administrative interface unless the factory-assigned administrative password has been changed by the user.	
IAM-008	An element SHOULD provide support (e.g., API) for integration with password managers to facilitate secure management of administrative passwords.	
IAM-009	An element SHALL support configuration of precedence of authentication methods.	
IAM-010	An element's identity is a global or network-unique device identifier that SHOULD be attestable.	
IAM-011	An element's identity SHOULD be attested through cryptographically strong mechanisms.	
IAM-012	An element SHALL provide a mechanism to securely deploy and update trust anchors.	
IAM-013	An element SHALL provide a mechanism to securely deploy and renew any device identifier and associated secrets used by the element.	
IAM-014	An element SHALL validate the status of any credentials, such as certificates or secrets.	
IAM-015	An element SHALL NOT use a secret such as a private or symmetric key in the clear for authentication.	
IAM-016	An element SHALL NOT use a credential that was not securely provisioned or installed.	
IAM-017	Element credentials SHALL have a validity period.	
IAM-018	A manufacturer SHOULD provide documentation on the quantum-resistant roadmap for their elements.	
IAM-019	An element SHALL provide support for using a centralized IAM platform.	
IAM-020	Identity providers SHALL follow the requirements as provided in [NIST 800-63C].	

6.2.1 IAM Requirements Clarifications

IAM-001

It is recommended to use a passphrase instead of a password. If a password is to be used, it is recommended that the password have a minimum length of 12 characters and not be easily guessable, and the maximum supported value should be no less than recommended by section 5.1.1.2 of [NIST 800-63B].

IAM-002

Refer to IAM-001 for guidance on password strength.

IAM-003

No further clarification.

IAM-004

Refer to section 5.1.1.2 of [NIST 800-63B] for guidance on password storage, salt size, hash function strength, and cost factor of key derivation functions.

It is recommended to not use deprecated hashing functions such as SHA1 or MD5.

IAM-005

When technical limitations render IAM-005 not possible, additional mechanisms should be put into place such as a privileged access management solution.

IAM-006

If a reusable password must be used, it must be stored, salted, and hashed and have a minimum length of 16 characters.

IAM-007

No further clarification.

IAM-008

No further clarification.

IAM-009

No further clarification.

IAM-010

The form of unique logical identifier is implementation specific.

IAM-011

The best practice for attestation is to use digital certificates. Other mechanisms can be considered in special situations.

IAM-012

Manufacturer/vendor needs to provide documentation for their mechanism(s).

IAM-013

This requirement does not require any automation. Device identifiers are used for element-to-element authentication and network provisioning.

Manufacturer/vendor needs to provide documentation for the mechanism(s).

IAM-014

For example, any available local or global credential validation mechanism(s) such as DBMS, CRLs lookup, or OCSP.

IAM-015

It is recommended that any services and traffic to HTTP be redirected to HTTPS. If a TLS domain certificate is not feasible, a self-signed certificate should be used.

IAM-016

For example, any available local or global credential validation mechanism(s) such as DBMS, CRLs lookup, or OCSP.

IAM-017

No further clarification.

IAM-018

No further clarification.

IAM-019

No further clarification.

IAM-020

No further clarification.

6.2.2 IAM Operators Common Practices

Administrative passwords should be stored and provisioned by operators on password managers to facilitate secure management of passwords.

Administrative passwords should be random and rotated. In the cases where an identity provider or AAA solution is unavailable, a locally unique credential can be used for console or craft interface access.

By default, locally configured password authentication shall always be the last choice.

6.3 Security Associations (SA)

6.3.1 Security Associations General (SA-GEN) Requirements

Table 3 - Security Associations General Requirements (SA-GEN)

REQ#	Description	Status/Comment
SA-GEN-001	All connections to an element SHALL use a secure channel.	
SA-GEN-002	An element SHALL NOT implement insecure services.	
SA-GEN-003	An element SHALL NOT use known weak security protocols or interfaces.	
SA-GEN-004	An element SHALL acquire time before determining the authentication and authorization requests.	
SA-GEN-005	An element SHOULD always verify that the source address of any emitted packets is appropriate for the element.	
SA-GEN-006	An element SHALL only use recommended and non-deprecated cipher suites.	

6.3.2 SA-GEN Requirements Clarifications

SA-GEN-001

Secure channel is authenticated, authorized, confidential, and integrity protected.

SA-GEN-002

Insecure channel is unauthenticated, unauthorized, non-confidential, or not integrity protected.

Examples of insecure services are chargen, TFTP, Telnet, and FTP services.

SA-GEN-003

Protocol or interface cannot use deprecated standards or implementations with known significant security weakness. This applies to authentication, authorization, encryption, and integrity mechanisms.

SA-GEN-004

When technical limitations render SA-001 not possible, element may bypass the time check and go to a probation mode. Authentication with acquired time will be performed when time is acquired.

SA-GEN-005

No further clarification.

SA-GEN-006

For TLS 1.3, it is recommended to use cipher suites as specified in [RFC 8446].

For TLS 1.2, it is recommended to use cipher suites as specified in [RFC 4492] and [RFC 5246].

For SSH, it is recommended to use cipher suites as specified in [RFC 9142].

6.3.3 Element Authentication (SA-EAN) Requirements

Table 4 - Element Authentication Requirements (SA-EAN)

REQ#	Description	Status/Comment
SA-EAN-001	An element SHALL support multi-factor authentication for administrative access.	
SA-EAN-002	An element SHALL implement mechanisms to prevent brute force login/access attacks as recommended in [NIST 800-63B].	
SA-EAN-003	An element SHALL require periodic reauthentication (or authentication) following any period that is configurable by the operator; the default value is that specified in [NIST 800-63B] by default.	
SA-EAN-004	An element SHALL renew authentication after an inactive period configurable by the operator; the default value is that specified in [NIST 800-63B] by default.	
SA-EAN-005	An element that provides access via an HTTP service SHALL use an encrypted channel such as TLS.	
SA-EAN-006	An element that uses TLS SHALL NOT use any deprecated versions of TLS.	
SA-EAN-007	An element that uses SSH SHALL NOT use any deprecated versions of SSH.	
SA-EAN-008	An element SHALL support 802.1X or equivalent mechanisms for wired and wireless network authentication.	

6.3.4 SA-EAN Requirements Clarifications

SA-EAN-001

The requirement for the element is to be able to support configuration of multi-factor authentication by the operator. See section 4.2.1 of [NIST 800-63B] for recommended multi-factor authenticator types. The vendor/manufacturer may require that the element be online in order to support multi-factor authentication.

SA-EAN-002

No further clarification.

SA-EAN-003

Refer to sections 4.3.3 and 7.2 of [NIST 800-63B] for recommended reauthentication timeout and periodic reauthentication.

SA-EAN-004

The session is terminated if a reauthentication attempt times out.

Refer to sections 4.3.3 and 7.2 of [NIST 800-63B] for recommended reauthentication timeout and periodic reauthentication.

SA-EAN-005

For example, many networks require support for Web UI, and this must be secured.

It is recommended that any services and traffic to HTTP be redirected to HTTPS. If a TLS domain certificate is not feasible, a self-signed certificate should be used.

SA-EAN-006

For more details on example deprecated versions, refer to [RFC 8996].

An element is strongly recommended to use TLS 1.3.

SA-EAN-007

Element needs to be compliant with [RFC 4250], [RFC 4251], [RFC 4252], [RFC 4253], and [RFC 4254].

SA-EAN-008

No further clarification.

6.3.5 Element Authorization (SA-EAZ) Requirements

Table 5 - Element Authorization Requirements (SA-EAZ)

REQ#	Description	Status/Comment
SA-EAZ-001	An element SHALL support the ability to restrict control plane access to authorized IP address space.	
SA-EAZ-002	Network elements SHALL support ingress and egress packet filtering of IPv4 and IPv6 packets.	
SA-EAZ-003	Network elements SHALL permit only required protocols and services necessary for the functions of the elements by default.	
SA-EAZ-004	An element SHOULD NOT require a user interactive approach (e.g., CLI) for configuring user and element access by default.	
SA-EAZ-005	An element SHALL provide a machine-to-machine interface for configuration and provision.	
SA-EAZ-006	An element that acts as a policy enforcement point (PEP) SHOULD provide a secure method to configure policies.	

6.3.6 SA-EAZ Requirements Clarifications

SA-EAZ-001

Authorized IP address space is defined as a set of well-known addresses (e.g., IP address) that are allowed to perform management operations according to the authorization policies.

SA-EAZ-002

Network elements will support sufficient ingress and egress packet filtering rules as necessary as the purpose of the elements.

SA-EAZ-003

No further clarification.

SA-EAZ-004

This requirement does not preclude the network element supporting a CLI for technician access.

SA-EAZ-005

Examples of machine-to-machine interface access include NETCONF or RESTCONF, etc.

SA-EAZ-006

To support dynamic policy enforcement, it is recommended that operators establish profiles based on attributes. Some examples of these attributes are listed below:

- temporal—outside of the normal window access;
- behavior—access to critical component(s); and
- geographical—access is not from a normal location the user used to access.

6.3.7 SA-EAZ Operators Common Practices

Access to an element shall be policy-based using role- or attribute-based access control.

Attribute-based access control (ABAC) model is preferred; see [NIST 800-162] for more guidance.

Policy-based access controls should enable the minimum privileges necessary.

6.3.8 User Authentication (SA-UAN) Requirements

Table 6 - User Authentication Requirements (SA-UAN)

REQ#	Description	Status/Comment
SA-UAN-001	An element SHALL support the AAA server solution for user authentication.	
SA-UAN-002	The AAA server SHALL support common muti-factor authentication (MFA) solutions that comply with [NIST 800-63B].	
SA-UAN-003	The AAA server SHALL support centralized credentials in addition to MFA compliant with [NIST 800-63B].	

6.3.9 SA-UAN Requirements Clarifications

SA-UAN-001

No further clarification.

SA-UAN-002

No further clarification.

SA-UAN-003

No further clarification.

6.3.10 User Authorization (SA-UAZ) Requirements

Table 7 - User Authorization Requirements (SA-UAZ)

REQ#	Description	Status/Comment
SA-UAZ-001	An element SHOULD disable by default any physical and/or logical communication ports that are not required for normal operation.	
SA-UAZ-002	An element SHALL NOT expose protocols meant to operate on north-bound network interfaces on its south-bound interfaces and vice versa.	
SA-UAZ-003	An element SHALL perform input validation to prevent improper resource use and typical injection attacks.	
SA-UAZ-004	An element SHALL NOT expose administrative access to/from the Internet by default.	
SA-UAZ-005	An element SHALL support key exchange algorithms that provide perfect forward secrecy (PFS).	
SA-UAZ-006	A network element's default configuration SHALL select encryption algorithms that provide authenticated encryption with additional data.	
SA-UAZ-007	A network element SHOULD support AEAD algorithms as specified in [RFC 5116].	
SA-UAZ-008	An element SHALL support disabling a given cipher suite.	
SA-UAZ-009	An element SHALL use cryptographic hash functions that are at least 128 security bits in strength or equivalent for any secure hashing or HMAC operations.	

6.3.11 SA-UAZ Requirements Clarifications

SA-UAZ-001

Such communication ports can be the console ports of the intelligent amplifier, wireless management interfaces, or remote management interfaces.

Note that the operator should be able to disable management interfaces required for configuration but not used in operation when no longer needed.

Certain protocols like SSDP/UPnP, mDNS, etc., are meant to be operated within a local network segment, and services utilizing such protocols should not listen and/or respond to on WAN and/or Internet-facing interfaces.

SA-UAZ-002

Certain protocols like SSDP/UPnP, mDNS, etc., are meant to be operated within a local network segment, and services utilizing such protocols should not listen and/or respond to on WAN and/or Internet-facing interfaces.

SA-UAZ-003

For examples of injection attacks, refer to "A03:2021-Injection" in [OWASP 10].

SA-UAZ-004

An element is expected to have multiple interfaces that includes ethernet, Wi-Fi, and virtualized interfaces. During normal operations, these interfaces may have different accessibility scopes:

- accessible only on a local/LAN IP subnet for the subscriber;
- accessible only on the WAN side by the network operator's infrastructure if it is also the operator management interface;
- accessible by any endpoint within certain physical proximity of the element (administrative access disabled by default); and
- accessible by any endpoint on the Internet (administrative access disabled by default).
- Note: If an ethernet interface is used for operator management of the element, administrative access should have access control on the interface.

It is important that operators have the ability to completely control exposure of the elements to management services. Also, elements should not be able to access services outside the management scope defined by the operators.

SA-UAZ-005

Key types recommended are elliptical-based algorithms. Use keys from curves in [NIST 800-56C]. Alternatively, use non-deprecated algorithms allowed by TLS 1.3.

SA-UAZ-006

Note that AES-CBC is not authenticated encryption.

SA-UAZ-007

For example, AES-GCM-SIV, which supports AEAD.

SA-UAZ-008

It is recommended that there be two different cipher suites supported for a given cryptographic function.

SA-UAZ-009

For example, SHA-256 and SHA3 (Keccak) are considered sufficient for 128 security bits in strength.

6.4 Asset Inventory and Management (AIM)

6.4.1 Asset Management and Inventory General (AIM-GEN) Requirements

Table 8 - Asset Management and Inventory General Requirements (AIM-GEN)

REQ#	Description	Status/Comment
AIM-GEN-001	An element SHALL support protocols (e.g., LLDP) for asset discovery.	
AIM-GEN-002	An element SHALL support automated methods aiding in asset inventory enrollment.	
AIM-GEN-003	An element SHALL allow use of its identity for asset management.	
AIM-GEN-004	An element SHALL provide a means to inventory assets that are retained on the element.	
AIM-GEN-005	A manufacturer SHALL provide hardening configuration templates and guidelines for elements.	

REQ#	Description	Status/Comment
AIM-GEN-006	A manufacturer SHALL provide environmental and operational assumptions. The assumptions need to include threat models that map out application, architecture, and infrastructure of the element as intended to be employed to provide a structured way to understand security protections and weaknesses.	
AIM-GEN-007	A manufacturer SHALL deliver products with proper hardening.	
AIM-GEN-008	An element SHALL be tested before implementing to the production environment.	
AIM-GEN-009	An element that is expected to be deployed in a location outside an operator's secure facility (e.g., subscriber's premises or OSP) SHALL include tamper-evidence capabilities.	
AIM-GEN-010	An element that is expected to be deployed in a location outside an operator's secure facility (e.g., subscriber's premises or OSP) SHALL include tamper-detection capabilities.	

6.4.2 AIM-GEN Requirements Clarifications

AIM-GEN-001

No further clarification.

AIM-GEN-002

This requirement is intentionally vague to allow operators to choose how they will support inventory processes.

AIM-GEN-003

For more details, see IAM-010 and IAM-011.

AIM-GEN-004

Assets that should be inventoried include but are not limited to management accounts, cryptographic keys or other primitives (particularly necessary for assessing cryptographic reediness for PQC transition), credentials or certificates, configuration files, licenses, or any other aspect of the element necessary for its intended function or to configure its operation.

AIM-GEN-005

No further clarification.

AIM-GEN-006

Refer to [NIST 800-154] for more guidance on threat modeling

AIM-GEN-007

Examples of providing proper hardening include using cryptographic strong methods for initial credentials for user or network, enabling default configuration to provide baseline security controls for elements, and properly patching the element.

AIM-GEN-008

Best common practices for operators to perform such a test include

- testing with a small group of customers/services/data,
- validating the element/DUT properly in a pre-configured test environment,
- validating of configuration as a code (see CCM section for more details), and
- removing sensitive data before the production implementation.

AIM-GEN-009

No further clarification.

AIM-GEN-010

Examples of tamper detection mechanisms include a light detector placed inside a hermetic enclosure or a mechanical switch to detect the opening of the element enclosure door.

6.4.3 Software Asset Management (AIM-SW) Requirements

Table 9 - Software Asset Management Requirements (AIM-SW)

REQ#	Description	Status/Comment
AIM-SW-001	All firmware or software updates and all security patches used in elements SHALL be digitally signed or use a similar integrity protected to an attestable root of trust.	
AIM-SW-002	An element SHALL provide downgrade protection to prevent unauthorized installation of a prior version of firmware.	
AIM-SW-003	A manufacturer SHOULD NOT use software components or library versions that have publicly known vulnerabilities of [CVSS] qualitative severity rating scale of medium or higher.	
AIM-SW-004	A manufacturer SHALL include vulnerability scanning for software components or library used on an element and provide remediation in both development and release workflow.	
AIM-SW-005	A manufacturer SHALL disclose known or discovered vulnerabilities to at least affected customers in a timely manner. Disclosure will include a severity rating and vulnerability summary, description, and impacts.	
AIM-SW-006	A manufacturer SHOULD provide mitigation instructions for disclosures as soon as practical.	
AIM-SW-007	A manufacturer SHALL maintain a list of all software components (software elements, libraries, etc.) used and provide a software bill of materials (SBOM) including each component that is conformant with [NTIA SBOM].	
AIM-SW-008	An element SHOULD use the version of component if the version of this component has no known vulnerabilities.	
AIM-SW-009	An element SHOULD use the most recent stable software components or library versions.	
AIM-SW-010	An element SHOULD support mechanisms to enforce operator's authorization of software updates and security patches.	
AIM-SW-011	An element SHALL always verify it has the operator's authorization to perform software updates and security patches before starting these processes.	
AIM-SW-012	A manufacturer SHOULD provide updates to upgrade any software components or libraries with known applicable security vulnerabilities in a timely manner.	
AIM-SW-013	A manufacturer SHALL train developers in application security concepts and secure coding, to include partners.	
AIM-SW-014	A manufacturer SHALL implement code-level security checks, applying static and dynamic analysis tools throughout the application life cycle to ensure secure coding practices are followed.	
AIM-SW-015	A manufacturer SHALL disclose the date for the end of support of the software components as soon as the date has been determined.	

6.4.4 AIM-SW Requirements Clarifications

AIM-SW-001

Refer to KEY-001 for recommendations on acceptable cryptographic functions for encryption and integrity protection. An example of integrity protection is using hash functions to verify the integrity of the firmware (e.g., SHA-256).

AIM-SW-002

Note that downgrade protection should not prevent rolling back to a previous working version if a new firmware version update is unsuccessful. Refer to [NIST 8259A] for guidance.

AIM-SW-003

Note that software components also include the underlying operating system, system libraries, and bootloaders. This is intended to apply to known vulnerabilities at the time of device firmware release. In certain circumstances (e.g., software components for legacy features or specialized capabilities), it is possible to not have feasible alternatives. Such situations need to be handled on a case-by-case basis.

Software version should be scanned prior to release.

AIM-SW-004

The specific methods for enforcement of this requirement are out of the scope of this document.

AIM-SW-005

The specific procedure and timeline for such disclosures are beyond the scope of this document. CISA has provided guidance to use VEX to report software vulnerabilities; see [CISA VEX]. Because of operators' distributed operations, it may be useful for vulnerabilities reported by manufacturers to be stored in a common repository by operators.

In line with the public policies from CISA, the expectation for timely disclosure is that network operators should be informed of vulnerabilities within a roughly 45-day window of discovery, regardless of whether a patch is available yet or not.

AIM-SW-006

No further clarification.

AIM-SW-007

It is recommended that this list be maintained in a machine-readable, commonly used format (e.g. [SWID], [SPDX], [CycloneDX]). The list may be provided to the operator as part of an agreement. Refer to [NTIA SBOM] for more detail.

Disclosure must minimally be available to the customers and may be available publicly.

AIM-SW-008

No further clarification.

AIM-SW-009

No further clarification.

AIM-SW-010

No further clarification.

AIM-SW-011

An example method is to use digital signature co-signing using a PKI certificate such as used in DOCSIS.

AIM-SW-012

It is recommended that any software components or libraries with known security vulnerabilities (either publicly provided or identified through internal process) be upgraded in the subsequent release. It is recommended that software components or libraries are always kept up to date in each release, regardless of known applicable security vulnerabilities, as part of life-cycle management, including avoiding software that is no longer supported. This reduces the difficulty of updates when a vulnerability is identified. The expectation is that this is handled on a case-by-case basis.

In line with the public policies from CISA, the expectation for timely disclosure is that network operators should be informed of vulnerabilities within a roughly 45-day window of discovery, regardless of whether a patch is available yet or not.

AIM-SW-013

No further clarification.

AIM-SW-014

No further clarification.

AIM-SW-015

The term "end of support of the software components" means the manufacturers stop providing security patches.

6.4.5 Hardware Asset Management (AIM-HW) Requirements

Table 10 - Hardware Asset Management Requirements (AIM-HW)

REQ#	Description	Status/Comment
AIM-HW-001	A manufacturer SHOULD provide information such as vulnerability scanning result, recommended configuration, and hardware bill of materials (HBOM) for operators to conduct internal assessments.	
AIM-HW-002	A manufacturer SHOULD disable all non-essential hardware-based consoles before product delivery.	
AIM-HW-003	An element SHOULD provide the ability to disable all non-essential hardware-based consoles.	
AIM-HW-004	A manufacturer SHOULD maintain a list of all hardware components used and follow the hardware bill of materials (HBOM) framework.	
AIM-HW-005	A manufacturer SHOULD disclose discovered hardware vulnerabilities or any known impacts to the hardware supply chain to operators in a timely manner.	

6.4.6 AIM-HW Requirements Clarifications

AIM-HW-001

No further clarification.

AIM-HW-002

The hardware console needs to be both electronically and physically disabled, and the ability to both manipulate the element and read the information from the element is prevented in production scenarios.

This requirement only applies to elements managed by operators.

AIM-HW-003

"Non-necessary" means such connectors or ports that are not needed for production services.

AIM-HW-004

For more details, see [CISA HBOM].

AIM-HW-005

In line with the public policies from CISA, the expectation for timely disclosure is that network operators should be informed of vulnerabilities within a roughly 45-day window of discovery, regardless of whether a patch is available yet or not.

6.4.7 Data Asset Management (AIM-DT) Requirements

Table 11 - Data Asset Management Requirements (AIM-DT)

REQ#	Description	Status/Comment
AIM-DT-001	An element SHALL support mechanism(s) to sanitize or destroy sensitive data before reselling or disposal.	
AIM-DT-002	An element SHALL support mechanisms to sanitize any sensitive data before being downgraded to a less sensitive classification.	
AIM-DT-003	An element SHOULD support mechanism(s) for preventing data exfiltration.	
AIM-DT-004	All sensitive data persistently stored on the element SHALL be encrypted.	

6.4.8 AIM-DT Requirements Clarifications

AIM-DT-001

Sensitive data refers to the information whose loss, misuse, or unauthorized access or modification could adversely affect security.

Examples of sensitive data include personally identifiable information (PII), intellectual property, shared secrets, private keys, certificates, consumer's data, etc. Refer to [NIST 8496 ipd] for more details.

AIM-DT-002

Refer to the clarification of AIM-DT-001 for details on sensitive data.

AIM-DT-003

Refer to KEY-001, KEY-002, and IAM-004 for information on protecting credentials and identities. For data on storage, it is recommended to use a [FIPS 140-3]-compliant version of a cryptographic library for data encryption and integrity check.

AIM-DT-004

Refer to the clarification of AIM-DT-001 for more details on sensitive data.

6.4.9 Account Asset Management (AIM-AC) Requirements

Table 12 - Account Asset Management Requirements (AIM-AC)

REQ#	Description	Status/Comment
AIM-AC-001	An element SHOULD support automated approaches for account management in accordance with dynamic role-based access policies.	
AIM-AC-002	An element SHOULD support mechanisms for the configuration of the time for temporary accounts to access.	
AIM-AC-003	An element SHALL reject access attempts or revoke the existing access for a temporary account once the pre-configured timer has been exceeded.	
AIM-AC-004	An element SHALL reject access attempts or revoke the existing access of an inactive account.	
AIM-AC-005	An element SHOULD support mechanisms of the discovery and inventory of any accounts that are actively used for managing this element.	

6.4.10 AIM-AC Requirements Clarifications

AIM-AC-001

"Dynamic" indicates that such policy should be periodically audited and updated.

AIM-AC-002

It is recommended to use a default configuration for the length of time that a temporary account can access the elements. This default value should be left to operators and vendors to decide.

AIM-AC-003

No further clarification.

AIM-AC-004

No further clarification.

AIM-AC-005

No further clarification.

6.5 Measurement and Attestation (MA)

6.5.1 Measurement and Attestation General (MA-GEN) Requirements

Table 13 - Measurement and Attestation General Requirements (MA-GEN)

REQ#	Description	Status/Comment
MA-GEN-001	When possible, an element SHALL acquire trusted time before performing the validity period or expiration checking.	
MA-GEN-002	An element SHALL support an automated approach for local or remote attestation.	
MA-GEN-003	An element SHALL NOT be allowed to pass customers' traffic to the network if it fails any requirements of measurement and attestation check listed in this section.	
MA-GEN-004	An element SHOULD upon failure send notification messages to management platform.	

6.5.2 MA-GEN Requirements Clarifications

MA-GEN-001

In the situations where an element needs to get access to the network first to acquire time, the validity period or expiration checking must be performed later with the acquired time in a pre-configured timeframe.

The local measurement and attestation approach also requires the integrity check of time. See more details in the MA-INT section, "integrity of time."

The definition of "trusted time" is out of the scope of this document.

MA-GEN-002

Examples of local or remote attestation include but are not limited to inspecting the signed logs or configuration during the boot process and sending it to a local/remote attestor to verify the behavior performed is as expected.

MA-GEN-003

Place this element in a walled garden or similar protected network (e.g., put the element in an isolated network) to allow remote troubleshooting.

MA-GEN-004

Refer to MA-GEN-003 for the definition of "failure."

6.5.3 Boot Security General (MA-BT) Requirements

Table 14 - Boot Security General Requirements (MA-BT)

REQ#	Description	Status/Comment
MA-BT-001	An element SHALL have a hardware root of trust that is used to validate the integrity and authenticity of the bootloader and firmware.	
MA-BT-002	The bootloader of the element which provides initial verification (e.g., FSBL) SHALL reside in non-reprogrammable memory.	
MA-BT-003	An element SHALL gracefully recover to a working state using the last known good image in the event a software upgrade fails without enabling image downgrade attacks.	

6.5.4 MA-BT Requirements Clarifications

MA-BT-001

In order to prevent situations where the element uses the wrong root of trust, i.e., one that has already been revoked or compromised, it is recommended to use multiple roots of trust configured by One Time Programmable (OTP) fuses within the Replay Protection Memory Blocks (RPMBs) or Trusted Execution Environments (TEEs).

MA-BT-002

This may be mask ROM, other one-time programmable, or internal flash protected by a security "fuse" to deny write. Any cryptographic material such as a hash or public key used for signature validation must also be in non-reprogrammable storage. Reprogramming will require special hardware and physical steps.

MA-BT-003

It is recommended that an element should keep at least two golden images for failure recovery.

6.5.5 Secure Boot (MA-SB) Requirements

Table 15 - Secure Boot Requirements (MA-SB)

REQ#	Description	Status/Comment
MA-SB-001	An element SHALL include support for secure boot with an unbroken chain of trust from ROM through all initialization stages, including boot code, operating system, firmware, drivers, and applications.	
MA-SB-002	An element SHALL implement secure boot using a multi-stage bootloader.	
MA-SB-003	An element SHALL implement rollback protection to prevent a vulnerable firmware version from being installed.	
MA-SB-004	An element SHOULD use One Time Programmable (OTP) bits for the anti-rollback mechanism.	
MA-SB-005	Once secure boot is enabled, an element SHALL always boot into a defined secure boot process and cannot boot into an unsigned/unsecured code or image.	
MA-SB-006	In dual boot systems, when secure boot is enabled, an element SHALL attempt to recover the device by booting the second system if the primary execution path fails.	
MA-SB-007	If the second boot sequence fails, an element SHALL provide an indicator that the element is unrecoverable.	
MA-SB-008	An element SHALL NOT execute code if any authentication or integrity check fails.	
MA-SB-009	A manufacturer SHALL provide support for all non-updatable code images to be PQ secure.	
MA-SB-010	A manufacturer SHALL provide a crypto-agile way for all updatable code images to allow upgrading to PQ keys and algorithms.	
MA-SB-011	An element SHALL double-bank all updatable images that are required to run to support software upgrades.	

6.5.6 MA-SB Requirements Clarifications

MA-SB-001

No further clarification.

MA-SB-002

The intention of this requirement is for the first stage bootloader to reside in ROM and to be as simple as possible to reduce the possibility of bugs. The subsequent, more complex, stages of the boot sequence would be updatable in the field. Storing the first stage bootloader in ROM helps to lock down the device and creates a hardware root of trust for the boot sequence.

MA-SB-003

No further clarification.

MA-SB-004

The anti-rollback mechanism should have write-access controls to grant or block access to groups of anti-rollback bits for different code images (e.g., it must be possible to configure the hardware such that the anti-rollback bits for the bootloader are only accessible for write operations by the bootloader).

MA-SB-005

This requirement is intended to apply to production environments only.

MA-SB-006

No further clarification.

MA-SB-007

No further clarification.

MA-SB-008

No further clarification.

MA-SB-009

No further clarification.

MA-SB-010

The upgrade mechanism shall be tested, and the test conditions and results shall be made available.

MA-SB-011

No further clarification.

6.5.7 Measured Boot (MA-MB) Requirement

Table 16 - Measured Boot Requirement (MA-MB)

REQ#	Description	Status/Comment
MA-SB-001	An element SHALL include support for secure boot with an unbroken chain of trust from ROM through all initialization stages, including boot code, operating system, firmware, drivers, and applications.	

6.5.8 MA-MB Requirement Clarification

MA-MB-001

No further clarification.

6.5.9 Integrity of Time (MA-TS) Requirement

Table 17 - Integrity of Time Requirement (MA-TS)

REQ#	Description	Status/Comment
MA-TS-001	An element SHALL support the capability to acquire time using a standards-based time protocol.	

6.5.10 MA-TS Requirement Clarification

MA-TS-001

Recommended protocols include NTP (see [RFC 5905], [RFC 8633], and [RFC 8915]) and PTP (see [IEEE 1588-2019]) secured with protocols such as MACsec.

6.5.11 Integrity of Configuration and State (MA-ICS) Requirements

Table 18 - Integrity of Configuration and State Requirements (MA-ICS)

REQ#	Description	Status/Comment
MA-ICS-001	Any data in non-volatile memory SHALL be encrypted.	
MA-ICS-002	Any data in flash memory SHALL be encrypted.	

6.5.12 MA-ICS Requirements Clarifications

MA-ICS-001

The recommendation is to encrypt all data including the firmware as well as operational/configuration data. Refer to KEY-001 for guidance on storage of encryption/decryption keys.

MA-ICS-002

See clarification of MA-ICS-001.

6.6 Security Information and Event Management (SIEM)—General Requirements

Table 19 - Security Information and Event Management General Requirements (SIEM)

REQ#	Description	Status/Comment
SIEM-001	An element SHALL support secure channels for transmission of all remote network management traffic.	
SIEM-002	An element SHALL support secure data collection and reporting mechanisms.	
SIEM-003	An element SHALL NOT support SNMPv1 or SNMPv2.	
SIEM-004	An element SHALL support logging of all administrative events.	
SIEM-005	An element SHOULD store logs for a configurable period of time.	
SIEM-006	An element SHALL NOT log any secret information, including but not limited to passwords, encryption keys, API keys, session keys, or other forms of credentials.	
SIEM-007	An element SHOULD support log signing.	
SIEM-008	An element SHALL support remote logging such as syslog or equivalent standard protocols over a secure channel such as TLS.	

6.6.1 SIEM Requirements Clarifications

SIEM-001

Refer to SA-GEN-001 and SA-GEN-006 for requirements of a secure channel.

Network management traffic includes configuration, telemetry data, and logging.

SIEM-002

When streaming telemetry cannot be used, it is recommended to use SNMPv3 for Security Information and Event Management.

For streaming telemetry protocols, it is recommended to secure them with TLS or SSH for real-time data collection.

For more details about requirements for TLS and SSH, refer to SA-EAN-006 and SA-GEN-006.

SIEM-003

No further clarification.

SIEM-004

Administrative events can result from changes/modifications to the operational configuration of the element and its services or can be notifications generated by the system in relation to the state of running processes. Some examples of administrative events are

- multiple failed login attempts, both remotely and locally;
- change of an administrative and/or user password;
- change in the firewall rules;
- change in the DNS or other network configuration;
- a process or service exits abnormally;

- privilege escalation, role change, or credential updates; and
- failure to fetch or sync time.

SIEM-005

Refer to section 4.2 in [NIST 800-92] for more examples of logging configuration settings.

For logs on storage, it is recommended to use a [FIPS 140-3]-compliant version of a cryptographic library for data encryption and integrity check.

SIEM-006

No further clarification.

SIEM-007

It is recommended to use [FIPS 186-5]- and [FIPS 180-4]-compliant algorithms for log signing.

SIEM-008

For more details on security considerations and best practices of Syslog, refer to [RFC 5424] and [RFC 5425].

6.7 Reliability and Availability (RA)

6.7.1 Reliability and Availability General (RA-GEN) Requirements

Table 20 - Reliability and Availability General Requirements (RA-GEN)

REQ#	Description	Status/Comment
RA-GEN-001	An element that provides multiple simultaneous login sessions SHALL limit administrators to one session per login credential.	
RA-GEN-002	An element SHOULD provide configuration to enable and disable the certificate validity checking to ensure the reliability of the service.	

6.7.2 RA-GEN Requirements Clarifications

RA-GEN-001

No further clarification.

RA-GEN-002

Refer to the SA section for authentication/authorization requirements for admins to perform this operation. Refer to SIEM-004 to make sure this behavior will always be logged.

6.7.3 Incident Response (RA-IR) Requirements

Table 21 - Incident Response Requirements (RA-IR)

REQ#	Description	Status/Comment
RA-IR-001	A manufacturer SHALL provide current contact information for reporting security incidents and issues and an escalation guide to include the CEO of the manufacturer.	
RA-IR-002	A manufacturer SHALL provide a process for reporting security incidents.	
RA-IR-003	A manufacturer SHALL provide documentation of their incident response process to operators.	
RA-IR-004	A manufacturer SHALL provide information on any security incidents and mitigations that would impact operators.	
RA-IR-005	A manufacturer SHALL maintain operator contact information for reporting security incidents.	
RA-IR-006	A manufacturer SHALL conduct post-incident reviews with operator incident management staff.	

6.7.4 RA-IR Requirements Clarifications

RA-IR-001

No further clarification.

RA-IR-002

No further clarification.

RA-IR-003

No further clarification.

RA-IR-004

No further clarification.

RA-IR-005

No further clarification.

RA-IR-006

No further clarification.

6.8 Configuration and Change Management (CCM)—General Requirements

Table 22 - Configuration and Change Requirements (CCM)

REQ#	Description	Status/Comment
CCM-001	An element SHALL receive any operational configurations over a secure channel.	
CCM-002	An element supporting advanced architectures such as virtual interfaces SHALL secure the virtual interfaces with the same controls as applied to physical interfaces to prevent unauthorized access.	
CCM-003	An element SHALL support enabling and disabling any service or protocol and all associated ports or interfaces, to include mDNS, UPnP, SSH, and Telnet (any version).	
CCM-004	An element SHALL NOT enable element management protocols on non-management interfaces.	
CCM-005	A manufacturer SHALL document all access methods (including any diagnostic access methods by supplier).	
CCM-006	An element SHALL support enabling/disabling all methods of access to the element (local and remote).	
CCM-007	An element SHALL support configurable login session timeout.	
CCM-008	An element SHALL support configurable inactivity timeout for login sessions.	
CCM-009	An element SHALL be able to reset to factory default deployment state, with all pre-reset customer and operator configuration data destroyed.	
CCM-010	An element SHALL support disabling remote access entirely.	
CCM-011	An element SHALL disable by default autorun and autoplay for active removable media ports (such as but not limited to USB).	

6.8.1 CCM Requirements Clarifications

CCM-001

Refer to SA-GEN-001 for the definition of secure channel.

CCM-002

No further clarification.

CCM-003

An element is expected to disable by default any services that are not required for the element to become operational. Additional services are to be enabled based on configured operational configuration. Services like mDNS, SSDP/UPnP, etc., that are meant operate within a subnet should not respond on management interfaces. Deprecated services like Telnet, FTP, and TFTP are to remain disabled on all interfaces.

CCM-004

Management protocols like TR-069, TR-369, and SNMP are not to be enabled on non-management interfaces.

CCM-005

This requirement is in conjunction with SA-UAZ-001 to ensure any access methods are disabled/secured by default.

CCM-006

This includes any mechanisms covered by SA-UAZ-001, CCM-002, and CCM-003.

CCM-007

No further clarification.

CCM-008

Refer to [NIST 800-63B] for a recommended default value for inactivity timeout.

CCM-009

The expectation is to ensure that any customer data (e.g., keys, passwords, confidential data) are cleared out and the element is in factory out-of-box state to be provisioned as a new element. This only refers to customer or provisioning data and does not restore to the previous software versions or software upgrades.

CCM-010

No further clarification.

CCM-011

This feature is very dangerous, and its misuse will result in a management Denial of Service or a compromise of the element.

Appendix I Acknowledgements

We wish to thank the following participants contributing directly to this document.

Contributor	Company Affiliation
Dusty Hoffpauir, Pawel Sowinski, Robert Hulshof, Saad Baig	Charter
Christopher Zarcone, Stephen Zevan, Ramsey Kraya, Chad Schieken	Comcast
David Taylor, Chris Sibley	Cox
Christian Corbin	Rogers
Yuan Tian, Steve Goeringer, Massimiliano Pala, Andy Dolan, Craig Pratt, Jason Rupe, Brian Scriber, Darshak Thakore, Gabby Gordon, Tao Wan	CableLabs

* * *