# CableLabs® Requirements
# CPE Security

# Common Security Requirements for IP-Based MSO-Provided CPE

# CL-RQ-IP-CPE-SEC-V01-130315

**RELEASED**

**Notice**

This CableLabs high-level requirements document is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides 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.

© Cable Television Laboratories, Inc. 2013

# DISCLAIMER

This document is published by Cable Television Laboratories, Inc. ("CableLabs®").

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 agencies; technological advances; or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. CableLabs makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the document or any information or opinion contained in the report. Any use or reliance on the information or opinion 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, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any cable member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such 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-RQ-IP-CPE-SEC-V01-130315 | | | |
| **Document Title:** | Common Security Requirements for IP-Based MSO-Provided CPE | | | |
| **Revision History:** | V01 – Released 3/15/13 | | | |
| **Date:** | March 15, 2013 | | | |
| **Status:** | ~~Work in Progress~~ | ~~Draft~~ | **Released** | ~~Closed~~ |
| **Distribution Restrictions:** | ~~Author Only~~ | ~~CL/Member~~ | ~~CL/ Member/ Vendor~~ | **Public** |

## Trademarks

CableLabs® is a registered trademark of Cable Television Laboratories, Inc. Other CableLabs marks are listed at http://www.cablelabs.com/certqual/trademarks. All other marks are the property of their respective owners.

# Contents



# Figures

# 1 SCOPE

## 1.1 Introduction and Purpose

MSOs are deploying devices to their customers' homes (and businesses) to provide various solutions - such as VoIP, video conferencing, security monitoring, home automation, energy monitoring, and medical monitoring. These devices, broadly referred to as CPEs (Consumer/Customer Premises Equipment) are to be managed by the MSO deploying them, and, based on the solution space in which they are used, must satisfy certain security and privacy concerns.

This document identifies the areas where common vulnerabilities exist for such CPEs, and crafts requirements to avoid those vulnerabilities.

It should be noted that most of the focus is on common vulnerabilities and security for how the operator manages the device. How the customers interact with the CPE, and security for such interactions, are out of scope.

Additionally, the requirements are categorized as "common" - those that apply to all classes of CPEs, and "solution-specific" - those that apply to specific classes of CPEs. For example, VoIP CPEs may have requirements that are not applicable to video camera CPEs. Such solution-specific requirements will be captured in individual appendices in future versions of this document.

## 1.2 Related work

### 1.2.1 DOCSIS

DOCSIS specifications (see [DOCSIS Security] and [DOCSIS BPI+]) cover security architecture and requirements for cable modems and VoIP equipment. Those specifications, however, do not cover the generic threat landscape for CPEs used in solutions mentioned above. Such CPEs may not be equipped with a DOCSIS credential, and thus may not be able to fulfill many of the architectural and functional requirements from the DOCSIS specifications.

### 1.2.2 TR-69

[TR-069] was created to have a common interface for managing a CPE. Thus, security of the device/its' platform itself is not the focus for [TR-069].

## 1.3 Assumptions

The solutions and requirements presented in this document make the following assumptions.

- The equipment this specification deals with is owned and provided by the operator, that is, NOT by the user.

## 1.4 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

| | |
|---|---|
| "must" | This word means that the item is an absolute requirement of this specification. |
| "must not" | This phrase means that the item is an absolute prohibition of this specification. |
| "should" | This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course. |
| "should not" | This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. |
| "may" | This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item. |

# 2 REFERENCES

## 2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[DOCSIS Security] DOCSIS 3.0 Security Specification, CM-SP-SECv3.0-I14-120809, August 9, 2012, Cable Television Laboratories, Inc.

[DOCSIS BPI+] DOCSIS Baseline Privacy Plus Interface Specification, CM-SP-BPI+-C01-081104, November 4, 2008, Cable Television Laboratories, Inc.

[TR-069] CPE WAN Management Protocol V1.1, Amendment 2, Broadband Forum, December 2007; http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf.

[NIST 800-133] Recommendation for Cryptographic Key Generation, NIST Computer Security Division, July 2011; http://csrc.nist.gov/publications/drafts/800-133/Draft-SP-800-133_Key-Generation.pdf

[AES] FIPS PUB 197, Advanced Encryption Standard, November 26, 2001; http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[RSA] PKCS #1: RSA Cryptography Standard v2.2, October 27, 2012; http://www.rsa.com/rsalabs/node.asp?id=2125.

[SHA-1] FIPS PUB 180-1, Secure Hash Standard, April 17, 1995; http://www.itl.nist.gov/fipspubs/fip180-1.htm.

[SHA-2] FIPS PUB 180-4, Secure Hash Standard, March 2012; http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

## 2.2 Informative References

This specification uses the following informative references.

[CWE] Common Weakness Enumeration: A Community-Developed Dictionary of Software Weakness Types, cwe-mitre.org.

[OWASP] Open Web Application Security Project, www.owasp.org

## 2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org

# 3 TERMS AND DEFINITIONS

This specification uses the following terms:

| | |
|---|---|
| **Multi-Factor Authentication** | Authentication requiring multiple (and potentially different types of) credentials. |
| **Role-Based Access Control** | An approach to access control where the privilege to perform an action on a particular resource is assigned to a "role", and individual users are assigned one or more roles. Privileges could be given to either coarse-grained actions or fine-grained actions. |
| **Fuzzing** | In software testing, fuzzing refers to the technique of testing with arbitrary data, in arbitrary sequence. The arbitrary data is typically crafted to be invalid (or unexpected). |

# 4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

| | |
|---|---|
| **AAA** | Authentication, Authorization and Auditing |
| **AES** | Advanced Encryption Standard |
| **BPI+** | Baseline Privacy Plus Interface |
| **CDP** | Cisco Discovery Protocol |
| **CM** | Cable Modem |
| **CMTS** | Cable Modem Termination System |
| **CPE** | Customer Premises Equipment |
| **CRL** | Certificate Revocation List |
| **CWE** | Common Weakness Enumeration |
| **DB** | Database |
| **DDoS** | Distributed Denial of Service |
| **DNS** | Domain Name Server |
| **DOCSIS** | Data-Over-Cable Service Interface Specifications - a suite of CableLabs specifications |
| **DoS** | Denial of Service |
| **FTP** | File Transfer Protocol |
| **HTTP** | Hyper Text Transfer Protocol |
| **ID** | Identifier |
| **IDE** | Integrated Development Environment |
| **IP** | Internet Protocol |
| **IPv4** | Internet Protocol Version 4 |
| **IPv6** | Internet Protocol Version 6 |
| **JSP** | Java Server Pages |
| **JTAG** | Joint Test Action Group |
| **LLDP** | Link Layer Discovery Protocol |
| **MFA** | Multi-Factor Authentication |
| **MSO** | Multiple Systems Operator |
| **MVPD** | Multiple Video Programming Distributor |
| **NIC** | Network Interface Card |
| **NIST** | National Institute of Standards and Technology |
| **NTP** | Network Time Protocol |
| **OCSP** | Online Certificate Status Protocol |
| **OS** | Operating System |
| **OWASP** | Open Web Application Security Project |
| **PIN** | Personal Identification Number |
| **QoS** | Quality of Service |
| **RBAC** | Role-Based Access Control |
| **RSA** | Asymmetric Encryption/Signature algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman |
| **SFTP** | Secure File Transfer Protocol |

| | |
|---|---|
| **SHA** | Secure Hash Algorithm |
| **SSH** | Secure SHell |
| **SSL** | Secure Socket Layer |
| **TACACS** | Terminal Access Controller Access-Control System |
| **TLS** | Transport Layer Security |
| **UTC** | Coordinated Universal Time |
| **VLAN** | Virtual Local Area Network |
| **WWW** | World Wide Web |

# 5 OVERVIEW OF A CPE DEVICE

In this section, a common definition of a CPE device is provided, along with how the rest of the document is structured.

## 5.1 CPE: Definition

A CPE device:

- is an IP device
- has a notion of some sort of OS, and software to support administrative interfaces (at a minimum)
- is deployed by an MSO into a customer's home or business
- is administered by the MSO using over-the-top protocols

In addition, a CPE device may

- have local storage capabilities
- support removable/external storage, and/or
- have additional ports

Note that core functionality provided by the CPE (video conferencing, for example), and the corresponding security requirements, are out-of-scope for the common requirements section. Solution-specific requirements will be covered in the solution-specific sections/appendices in future versions of this document.

Given below is a pictorial representation of a CPE device.

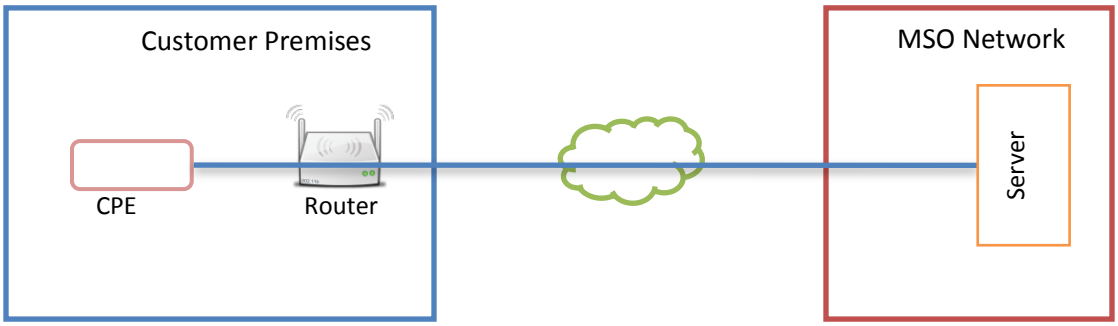


***Figure 1 - CPE deployment***

NOTE: Some of the connections into the device may originate from a human user, in addition to software running on a server in the MSO network.

The following picture identifies the composition of a CPE device (as relevant to this document).

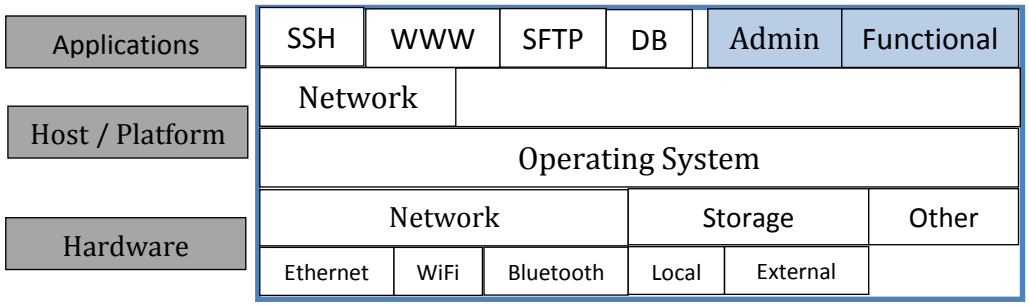


***Figure 2 - Composition of a CPE***

## 5.2 Threats

With Figure 2 above as a reference, the following threats (not a complete set) could exist.

1. Data: Data stored in the device or in transit could be compromised, in a number of ways.
   a. Physical access
      i. Copying the data using other storage interfaces supported
      ii. Hardware disassembly
   b. Network access, through
      i. Not implementing access restrictions based on roles
      ii. Application/services/OS vulnerabilities (like SQL Injection, buffer overflows, session hijacking, etc.)
      iii. Snooping network traffic (due to lack of confidentiality, integrity and/or authentication)
2. Availability: The network interfaces could be attacked using common IPv4 or IPv6 attack vectors, leading to general availability issues. Examples include DoS, DDoS, and fuzzing.
3. MSO Network: Unauthorized access to a CPE (through vulnerabilities identified above, or other vulnerabilities) could expose the MSO network to the attackers.

## 5.3 Requirement Categories

Given the above threats, this document is aimed at capturing the safeguards the cable industry wants to put in place in the CPE devices they would deploy.

These requirements are divided into the following categories.

- Hardware security
- Network security
- Software security
- Administrative interface security
- Storage security (internal/removable/external)
- Diagnostics/Troubleshooting mechanisms

In addition, generic requirements are captured in Section 6.7.

## 5.4 Out of Scope

Specifically, the following are out of scope:

- Router connectivity: There may be vulnerabilities in how the device connects to the router. However, this document does not focus on these issues.
- Discovery/Device addressability: After a device is deployed, it needs to be recognized by the server in the MSO network (as probably belonging to a specific customer), and the server may need a specific means to communicate with this particular device. However, this specification does not cover these areas (other specifications or custom procedures may be used). For example, BPI+ is a CableLabs specification (in the family of DOCSIS specifications) for CMs to register and securely communicate with a CMTS.
- Customer interaction with CPE: The security of access control to the device itself by the customer is out of scope.

# 6 COMMON REQUIREMENTS

This section captures common requirements that apply to all classes of CPE devices.

## 6.1 Hardware Requirements

This section discusses hardware and connectivity that the CPE must provide and related security requirements.

CPEs must provide some form of IP connectivity (Ethernet / 802.11a/b/g/n/ac). It is expected that CPEs put in place sufficient safeguards for standard network stack threats. It is also expected that the CPE handles such threats, when they occur, in a fail-safe manner (not causing interruptions to the core functionality). CPE manufacturers must provide documentation detailing the measures they have implemented to comply with the following requirements.

All hardware diagnostic interfaces, such as JTAG, must be disabled. This will ensure that a physical access does not allow an attacker to "plug into" the device and compromise data.

CPE must support the physical or logical disablement of any local console ports.

The vendor must not install or permit undocumented, unmonitored (i.e., backdoor) modes of communication to the device. Such communications may not be secured properly and thus have vulnerabilities, and/or could be exploited in unauthorized fashion.

## 6.2 Network Requirements

CPE must fully support both IPv4 and IPv6 in all applicable communications layers (network, transport, and application). This is to preserve availability of security frameworks across multiple network stacks (example: if SSH is reachable via IPv4, then it should be reachable via IPv6 as well).

CPE must support UTC synchronization via a centralized time protocol such as NTP. Note that this is critical, as accuracy of cross-referencing of log entries across all systems is important for audit and forensic purposes.

CPE must support DNS for hostname resolution.

CPE must be capable of withstanding a direct attack (such as DoS, DDoS, and fuzzing) without bringing down services or allowing additional functionality access to the device. This may be achieved through the use of access control techniques such as host-based firewalls and platform hardening. Other examples include appropriate log file rotation and size management.

The access control policies employed to withstand any attacks (DoS/DDoS, for example) must be configurable. In order to be able to enforce / customize network security policies, the CPE:

1. must support stateful network-layer access control, with a granularity of not less than traditional 5-tuple (source network address, source transport, destination network address, destination transport, protocol).
2. should have the ability to base access control decisions on any field in data-link, network or transport headers.
3. should have the ability to base access control decisions on direct inspection of application-layer payload.

CPEs must provide an administrative interface to manage these settings.

## 6.3 Software Security Requirements

The OS and software used in the CPE must also be secured against common threats. Since the CPE is connected to the internet and provides services reachable over the internet, safeguards against common software threats and service/port threats (like HTTP) must be put in place.

CPE vendors must provide documentation detailing the operating system and services they have installed on the device. Only minimal services should be installed [NIST 800-133].

All unnecessary system and network services must be disabled or removed.

CPE must support enabling/disabling of individual system and network services through some administrative interface. Additionally, the enablement of network discovery protocols (such as CDP, LLDP, Bonjour, etc.) must be configurable.

CPE operating system must support a mechanism to ensure memory, file system and binary integrity.

CPE must provide provisions for secure patch management of OS and the software used. Application and platform code must be digitally signed, and the signatures verified before installing that code.

CPE must not have the ability to compile or recompile any of the services; for example, remove kernel code used for compiling the OS or module sources used for compiling any services, and for Linux/Android based OSs, remove OS sources.

All development materials (source code, compilers, disassemblers, debuggers, IDEs, compile and link artifacts, symbol tables, uncompiled JSPs, etc.) must be removed from the CPE prior to delivery.

CPE must enforce the principle of least privilege for all services running on the device. This principle dictates that each task, process, or user is granted the minimum rights required to perform its job. Ideally, each service should run as a unique user ID. Accordingly, granular privileges must be used for user IDs used by each service, so that separation of privilege could be configured.

CPE manufacturers must itemize all classes of data processed by the CPE.

CPE must validate all input and ensure that appropriate bounds checking is performed on all input. Refer to [OWASP] Top Ten Project. Note that applications should be aware of attacks like fuzzing, and especially guard against DoS attempts at the application layer.

CPE software and firmware shall be reviewed for known programming errors that could potentially give rise to security vulnerabilities. Either automated or manual review is acceptable. Review should focus on common classes of errors (e.g., failure to validate input) as defined by authoritative sources like [CWE] and [OWASP].

CPE must fail gracefully when experiencing errors or exceptions. As an example, give some indication to the user that the system has failed, possibly with some error code and troubleshooting hints, as opposed to a blue screen of death.

CPE must avoid disclosing unnecessary design/implementation details to potential attackers (for example, through a stack trace or memory dump.)

## 6.4 Administrative Security Requirements

All CPE devices must provide some means for the MSO operators to administer the device. Typically, such administration is initiated over the network, using common protocols. Example protocols include SSH, Web, and (S)FTP. All administrative access must require a login. Login accounts may be managed on the device, or centralized AAA systems may be used. The network connection used for administration must also be secured and authenticated. Note that traffic could originate at the CPE or at the MSO back-office server. In either case, appropriate authentication of the source must be performed.

CPE must provide a way to administer the device. Examples include SSH, web interfaces, and Secure File Transfer Protocol (SFTP).

### 6.4.1 Administrative Interface Network Security

In order to preserve CPE administrative functions during network congestion, CPE must allow separation of administrative traffic from all other (functional) network traffic. This may be achieved by providing discrete physical (example: dedicated NIC) or logical (example: QoS, VLAN, DOCSIS service flow) interfaces. CPEs must provide one of the following:

- Logical separation of administrative traffic
- Hardware based separation of administrative traffic

All protocols used for administration must support transport encryption and strong authentication. Example protocols include TLS and SSH. Mutual authentication should be implemented. Where mutual authentication is

supported, CPE must support configuration of the credentials used for mutual authentication. For example, such credentials may be:

- Installed during manufacturing time
- Installed by a privileged user through an administrative interface

CPE must implement industry or *de facto* standard encryption algorithms (such as [AES] and [RSA]) and message digest algorithms, like [SHA-1] or [SHA-2].

Digital certificates, when used, must be issued from authorized certificate authorities. Demonstration or self-signed certificates are not permitted. Certificates must be unique per device.

CPE must support CRL verification and OCSP when verifying the client or server certificates. Additionally, CPE must support configuration of the validation parameters.

CPE must follow best practices for the generation and usage of cryptographic key material (including entropy and key size) as defined by standards bodies such as National Institute of Standards and Technology (NIST). (Refer to [NIST 800-133] for details.)

CPE must support termination of administrative sessions after a configurable period of inactivity.

### 6.4.2 Administrative Accounts/Logins

Default user, application, and system accounts must be disabled or renamed prior to production deployment.

CPE must fully support external centralized authentication, authorization and accounting, for administrative logins. Examples include Radius, Diameter and TACACS+.

CPE must support local account creation/configuration and logins using those local accounts.

If passwords are used as credentials for internal or local accounts, the CPE must support configurable password policies. The CPE must enforce following rules on the passwords, and the configuration of these rules must be customizable.

- Minimum length (example: not less than 8 characters)
- Minimum complexity (includes minimum thresholds for upper, lower case letters, numeric characters and special characters)
- Maximum age
- Minimum history

CPE must allow logins using local accounts ONLY when remote/central authentication servers are not reachable.

CPE must support at least one form of Multi-Factor Authentication (MFA) during administrative account login. The intent is to move beyond password and/or shared secret authentication. One example is digital certificates. The root of trust for digital certificates must be configurable. For example,

1. Such roots may be pre-installed at manufacturing time.
2. A privileged user may configure such root certificates through an administrative interface.

During login, CPE must display a configurable warning banner on any administrative interface prior to authentication.

CPE must not explain authentication failures with specificity (example, "The password was incorrect").

During login, visible display of passwords, PINs and any other authenticators should be suppressed.

CPE must support Role-Based Access Control (RBAC) to authorize functions performed using the administrative interfaces.

CPE must enforce the principle of least privilege for all administrative account. This principle dictates that each user/role is granted the minimum rights required to perform its job. Accordingly, granular privileges must be used in applications, so that separation of privilege can be configured.

CPE must provide a mechanism to display a complete list of all possible configuration settings and their current values. This must include values for any hidden configurations. It must be possible to display all values, even those that are disabled, "off", or set to default values.

## 6.5 Storage Security Requirements

Passwords, PINs, secret keys, private keys, and other authenticators must not be stored as plain text.

CPE manufacturers must supply detailed explanation as to how data is stored within the CPE.

Removable media (such as USB flash drives, compact flash and SD cards) must be securable via encryption and strongly-authenticated methods. CPE should provide administrative provisions to configure which data must be encrypted and which data need not be encrypted.

Access to data, from any interface (SSH, USB, Application, etc.) must be access controlled - meaning, access is allowed only after authentication and ensuring appropriate privileges.

## 6.6 Diagnostics/Troubleshooting Requirements

CPE should support centralized event logging, like syslog.

CPE that cannot support centralized logging must meet all of the centralized logging requirements locally.

At a minimum, the following events (successful or failed) must be logged.

- Remote access (authentication)
- Configuration changes

## 6.7 General Requirements

If the CPE asserts compliance with an industry standard (such as CableLabs, IETF, NIST, or Broadband Forum), it must implement the ENTIRE standard. Selective implementation of industry standards is not permitted.

CPE manufacturers must supply detailed connectivity matrices for all data flows associated with the device, including but not limited to data link protocols, network protocols, transport protocols, ports, directionality of data transmission, and the nature of data transmitted. For example, such information could be provided as a 5-tuple (source network address, source transport, destination network address, destination transport, protocol).

CPE manufacturers must supply full documentation for any proprietary protocols utilized.

# Appendix I Acknowledgements

We wish to heartily thank the following MSO participants who contributed directly to this document.

Christopher Zarcone (Comcast)

Amine Brahimi (Comcast)

Tom Johnson (Comcast)

Sailata Reddy (Comcast)

*Seetharama Rao Durbha, CableLabs*