Abstract: This document provides implementation guidance for securing Hardcopy Devices using existing network security and system management protocols, local secure peripherals, and system architecture approaches that support channel isolation and process isolation.

This is a PWG Working Draft. For a definition of a "PWG Working Draft", see:


This document is available electronically at:

The material contained herein is not a license, either expressed or implied, to any IPR owned or controlled by any of the authors or developers of this material or the Printer Working Group. The material contained herein is provided on an “AS IS” basis and to the maximum extent permitted by applicable law, this material is provided AS IS AND WITH ALL FAULTS, and the authors and developers of this material and the Printer Working Group and its members hereby disclaim all warranties and conditions, either expressed, implied or statutory, including, but not limited to, any (if any) implied warranties that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.
## Table of Contents

1. Introduction .................................................................................................................. 6

2. Terminology .................................................................................................................. 7

2.1 Conformance Terminology ......................................................................................... 7

2.2 Hardcopy Device Terminology ................................................................................... 7

2.3 Security Terminology .................................................................................................. 7

2.4 Protocol Role Terminology ......................................................................................... 8

2.5 Acronyms and Organizations ...................................................................................... 8

3. Rationale ....................................................................................................................... 10

3.1 Use Cases .................................................................................................................... 10

3.1.1 Managed IT Environment Using Health Assessment Protocols ............................ 10

3.1.2 IT Environment That Requires Common Criteria Certification ......................... 10

3.1.3 IT Environment That Requires Policy Enforcement Certification ....................... 11

3.2 Exceptions .................................................................................................................. 11

3.3 Out of Scope ............................................................................................................... 12

3.4 Design Requirements .................................................................................................. 12

4. HCD Network Security .................................................................................................. 13

4.1 Internet Suite and other Protocols .............................................................................. 13

4.2 Datalink Layer ........................................................................................................... 13

4.3 Network Layer ........................................................................................................... 13

4.4 Transport Layer ......................................................................................................... 13

4.5 Session Layer ............................................................................................................ 13

4.6 Presentation Layer ...................................................................................................... 13

4.7 Application Layer ....................................................................................................... 13

5. HCD Local Security ....................................................................................................... 13

5.1 Operating Systems and Hypervisors .......................................................................... 13

5.2 Local Secure Peripherals ........................................................................................... 13

5.3 Local Secure Applications ......................................................................................... 13

6. HCD System Architecture ............................................................................................ 13

6.1 Channel Isolation ......................................................................................................... 14

6.1.1 Firewalls ................................................................................................................. 14

6.1.2 AntiVirus Scanners ............................................................................................... 14

6.1.3 Malware Scanners ................................................................................................. 14

6.2 Process Isolation ......................................................................................................... 14

6.2.1 Sandboxes .............................................................................................................. 14

6.2.2 Containers ............................................................................................................. 14

6.2.3 Virtual Machines .................................................................................................... 14

7. Conformance ................................................................................................................ 14

8. Internationalization Considerations ............................................................................ 14

9. Security Considerations ............................................................................................... 14

10. References .................................................................................................................. 15

11. Authors’ Addresses ..................................................................................................... 27

12. Appendix A – Internet Protocol Suite ........................................................................ 27

12.1 Internet Protocol Suite Evolution ............................................................................. 27

12.2 Datalink Layer .......................................................................................................... 28

12.2.1 ARP ..................................................................................................................... 28
12.2.2 DHCP
12.2.3 Ethernet
12.2.4 MACsec
12.2.5 MKA
12.2.6 VLAN
12.2.7 Wi-Fi
12.2.8 WPA2
12.2.9 WPA3
12.3 Network Layer
12.3.1 ICMP
12.3.2 IP
12.3.3 IPsec
12.3.4 NAT
12.4 Transport Layer
12.4.1 TCP
12.4.2 TLS/DTLS
12.4.3 UDP
12.5 Session Layer
12.5.1 ICE
12.5.2 HTTP
12.5.3 STUN
12.5.4 TURN
12.6 Presentation Layer
12.6.1 ASN.1
12.6.2 CBOR
12.6.3 CDDL
12.6.4 HTML
12.6.5 JSON
12.6.6 REST
12.6.7 SGML
12.6.8 Unicode
12.6.9 UTF-8
12.6.10 UTF-16
12.6.11 UTF-32
12.6.12 XML
12.6.13 XSD
12.6.14 YANG
12.7 Application Layer
12.7.1 DNS
12.7.2 FTP
12.7.3 HTTP
12.7.4 IMAP
12.7.5 IPP
12.7.6 LDAP
12.7.7 MQTT
12.7.8 NETCONF
122  12.7.9 NTP .................................................................36
123  12.7.10 POP ..............................................................36
124  12.7.11 RESTCONF ..................................................37
125  12.7.12 SIP ..............................................................37
126  12.7.13 SMIv1 .........................................................37
127  12.7.14 SMIv2 ..........................................................37
128  12.7.15 SMTP ...........................................................37
129  12.7.16 SNMP ...........................................................38
130  12.7.17 SSH .............................................................38
131  12.7.18 Syslog ..........................................................38
132  12.7.19 Telnet ..........................................................39
133  13. Change History .................................................39
134  13.1 20 January 2020 ................................................39
135  13.2 31 December 2019 ............................................39
136  13.3 11 July 2019 .....................................................40
137  13.4 13 February 2019 ..............................................40
138
139
140
141  Figure 1 - An Example Figure ......................................6
142
143
144
145  Table 1 - An Example Table .........................................6
146
147
1. Introduction

This document provides implementation guidance for securing Hardcopy Devices using existing network security and system management protocols, local secure peripherals (e.g., TCG Trusted Platform Module [TCGTPM] and TCG OPAL Self-Encrypting Drive [TCGSED]), and system architecture approaches that support channel isolation and process isolation (e.g., sandbox, container, and virtual machine).

This document was inspired by the original IEEE Standard for Information Technology: Hardcopy Device and System Security [IEEE2600] and is intended to complement the current Common Criteria HCD-Protection Profile for Hardcopy Devices [HCDPP].
2. Terminology

2.1 Conformance Terminology

Capitalized terms, such as RECOMMENDED, SHOULD, SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as defined in Key words for use in RFCs to Indicate Requirement Levels [BCP14]. The term CONDITIONALLY RECOMMENDED is additionally defined for a conformance recommendation that applies when a specified condition is true.

2.2 Hardcopy Device Terminology

This document imports or generalizes the following Hardcopy Device terms from IETF Printer MIB v2 [RFC3805], IETF Finisher MIB [RFC3806], IETF Internet Printing Protocol/1.1 [STD92], and PWG MFD Model and Semantics [PWG5108.1].

Document: An object created and managed by a Hardcopy Device that contains description, processing, and status information. A Document object may have attached data and is bound to a single Job.

Job: An object created and managed by a Hardcopy Device that contains description, processing, and status information. The Job also contains zero or more Document objects.

Logical Device: A software implementation of an endpoint device (e.g., a print server, software service, or gateway) that processes Jobs and either forwards or stores the processed Jobs or uses one or more Physical Devices to render output.

Output Device: a single Logical or Physical Device.

Physical Device: a hardware implementation of an endpoint device (e.g., a Printer, Scanner, Fax, MFD, or other HCD).

2.3 Security Terminology

This document imports or generalizes the following security terms from [IEEE2600] and [PWG5110.1]:

Administrator: A user who has been specifically granted the authority to manage some portion or all of the HCD and whose actions may affect the security policy. Administrators may possess special privileges that provide capabilities to override portions of the security policy. [IEEE2600]

Application: Persistent computer instructions and data placed on the HCD, via download or additional hardware (e.g., daughter card), that are separate from, and not a part of, the base Firmware. Applications are an addition to the base Firmware that provide additional function beyond that provided by the base Firmware. [PWG5110.1]

Correlated Attributes: An ordered set of related attributes that describe an instance of firmware or software. The purpose of these Correlated Attributes is to allow ease-of-access and verification for each code instance. [PWG5110.1]
**Device Administrator**: A user who controls administrative operations of the HCD other than its network configuration (e.g., management of users and resources of the HCD). [IEEE2600]

**Firmware**: Persistent computer instructions and data embedded in the HCD that provides the basic functions of that device. Firmware is only replaced during a specialized update process. [IEEE2600]

**Hardcopy Device (HCD)**: A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, multifunction peripherals (MFPs), multifunction devices (MFDs), all-in-ones, and other similar products. [IEEE2600]

**Network Administrator**: A user who manages the network configuration of the HCD. [IEEE2600]

**Resident Application**: Resident applications are those applications that are downloaded via an offline administrative or maintenance update procedure and persist after a power cycle of the HCD. These types of applications augment the normal operation of the HCD and provide additional functions that are available to all users of the HCD. [PWG5110.1]

**User**: An entity (human user or IT entity) outside the HCD that interacts with the HCD. [IEEE2600]

**User Application**: User applications are applications that are downloaded and executed as part of normal operation of the HCD and may be dynamically installed and executed by users. These applications do not include applications that are added via an offline administrative or maintenance update procedure. Examples of these types of applications include Java or Flash applications. User applications may or may not persist after a power cycle of the HCD. [PWG5110.1]

### 2.4 Protocol Role Terminology

This document also defines the following protocol roles in order to specify unambiguous conformance requirements:

**HCD Client**: Initiator of outgoing connections and sender of outgoing imaging operation requests (Hypertext Transfer Protocol -- HTTP/1.1 [RFC7230] User Agent).

**HCD System**: Listener for incoming connections and receiver of incoming imaging operation requests that represents one or more Physical Devices or a Logical Device.

**HCD Agent**: Listener for incoming management requests and sender of optional outgoing notifications for a Hardcopy Device (e.g., an SNMP Agent).

**HCD Manager**: Initiator of outgoing management requests and receiver of optional incoming notifications for a Hardcopy Device (e.g., an SNMP Manager).

### 2.5 Acronyms and Organizations

**IANA**: Internet Assigned Numbers Authority, [http://www.iana.org/](http://www.iana.org/)


3. Rationale

Hardcopy Devices typically do not include the same software infrastructure and patch management mechanisms deployed in PCs or network servers. Hardcopy Devices in the past often did not include local system anti-virus programs, local system firewalls, local system intrusion detection, or other basic security infrastructure.

3.1 Use Cases

The following use cases are imported from section 3.2 of [PWG5110.1].

3.1.1 Managed IT Environment Using Health Assessment Protocols

A corporate IT department has decided to implement a network health assessment infrastructure as part of a rollout of laptop and desktop refresh for the company’s employees. The motivation behind the decision to implement an assessment protocol was driven by the increasing number of laptops used by employees that were used away from the office on unmanaged networks and only occasionally attached to the corporate network. These laptops could not automatically have their security patches, antivirus definitions etc. updated since they were not on the network when the administrator’s system management software executed batch updates.

Because Hardcopy Devices do not always support the network health assessment protocols, the IP address of each HCD is manually entered into an exception table with the health assessment scheme’s configuration tool. Industrious employees have discovered that they can program their laptops with the same IP address as the area’s shared printer and access the corporate network without having to manually install operating system patches and antivirus updates before being allowed access. Having HCDs report attributes would remove the need for most exceptions and therefore decrease the chance of unprotected laptops spreading malware.

3.1.2 IT Environment That Requires Common Criteria Certification

IT Security and Network administrators that follow specific Information Security Management System (ISMS) guidelines may require that all devices that attach to a network be certified via some external body, (e.g., Common Criteria). These certifications are usually only valid if the device is maintained in a particular configuration. For Hardcopy Devices, configuration parameters that may affect the status of a certification can include, but are not limited to:

- The specific level of firmware that is loaded into the HCD.
- The specific hardware ports that are enabled or disabled on the HCD.
- The specific network protocols that are enabled or disabled on the HCD.
- The specific port numbers that are enabled or disabled on the HCD.
- The specific services that are enabled on the HCD.
Any modification to these configuration parameters can result in the device no longer operating in its certified configuration.

3.1.3 IT Environment That Requires Policy Enforcement Certification

Organizations may have a set of internal policies that must be satisfied before a device is allowed on the network. Often these policy requirements are configuration requirements and may not seem directly related to "health." However, from the following example, it may be seen that configuration settings may be important elements for assessing the fitness of a device to attach to the network.

Users have discovered that they can gain access to the network by acquiring the address of a device on the exception list and statically assigning this IP address to their computer. Their computer is now on the exception list and is granted access. To mitigate this breach, IT administrators decide corporate policy is that ALL devices must acquire their IP addresses from a DHCP server. The configuration setting that enables/disables DHCP becomes part of the Policy Enforcement health assessment.

Policy Enforcement can encompass a wide range of configuration settings. The relevance of these settings may also vary between organizations. Some additional configuration elements that could be part of a policy statement include, but are not limited to:

- Secure Time Source
- Valid X.509 certificate signed by corporate Certificate Authority
- MAC addresses -- Universally Administered Address (UAA) versus Locally Administered Address (LAA)
- Enabled/Disabled protocols -- for example, no FTP daemon, or support for HTTPS but not for HTTP.
- Installed features -- for example, disallow printers with hard disks unless they support disk wiping.
- Authentication settings -- Kerberos/LDAP configuration
- Network proxy configuration
- DNS server address(es)

It is also important to note that some policy related settings, like disabled protocols and installed features, may overlap with other health related evaluations.

3.2 Exceptions

TBD
3.3 Out of Scope

The out-of-scope requirements for this HCD Security Guidelines document are:

1) Configuration of network security services and policies directly through the IPP System Service [PWG5100.22] or other PWG protocol.

2) Configuration of local security services and policies directly through the IPP System Service [PWG5100.22] or other PWG protocol.

3) Configuration of local peripheral security and policies directly through the IPP System Service [PWG5100.22] or other PWG protocol.

4) Configuration of local communications channel and process isolation security and policies directly through the IPP System Service [PWG5100.22] or other PWG protocol.

3.4 Design Requirements

The design requirements for this HCD Security Guidelines document are:

1) Define conformance recommendations that are consistent with [PWG5110.1].

2) Define conformance recommendations that are consistent with [PWG51100.4].

3) Follow the naming conventions used in [PWG5110.1].

4) Define conformance recommendations for network security that include: network time sources (e.g., NTP); public key infrastructure (e.g., LDAP); network name services (e.g., DNS); network security policy services (e.g., RADIUS); network directory services (e.g., LDAP); and network authentication services (e.g., Kerberos and OAuth2).

5) Define conformance recommendations for local security that include: …
4. HCD Network Security

This section addresses network security issues for HCDs, including wired and wireless access, Internet Suite protocols, and open standard system management protocols that can be used to secure Hardcopy Devices.

4.1 Internet Suite and other Protocols

4.2 Datalink Layer

4.3 Network Layer

4.4 Transport Layer

4.5 Session Layer

4.6 Presentation Layer

4.7 Application Layer

5. HCD Local Security

This section addresses local security issues for HCDs, including operating systems, peripherals, and applications.

5.1 Operating Systems and Hypervisors

5.2 Local Secure Peripherals

5.3 Local Secure Applications

6. HCD System Architecture

This section addresses system architecture approaches to enhance security of HCDs and by supporting channel isolation and process isolation, including sandboxes, containers, virtual machines, and hardware protected cryptographic engines.
6.1 Channel Isolation

6.1.1 Firewalls

6.1.2 AntiVirus Scanners

6.1.3 Malware Scanners

6.2 Process Isolation

6.2.1 Sandboxes

6.2.2 Containers

6.2.3 Virtual Machines

7. Conformance

TBD

8. Internationalization Considerations

Note: The following boilerplate text may not be sufficient for all purposes. In a standards-track working draft we include conformance requirements (see the wd-template file for details).

For interoperability and basic support for multiple languages, conforming implementations support:

- The Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [STD63]
- encoding of Unicode [UNICODE] [ISO10646]; and
- The Unicode Format for Network Interchange [RFC5198] which requires
- transmission of well-formed UTF-8 strings and recommends transmission of
- normalized UTF-8 strings in Normalization Form C (NFC) [UAX15].

Unicode NFC is defined as the result of performing Canonical Decomposition (into base characters and combining marks) followed by Canonical Composition (into canonical composed characters wherever Unicode has assigned them).

9. Security Considerations

Provide security considerations for this white paper.
10. References


W. George, C. Donley, C. Lijenstolpe, L. Howard, “IPv6 Support Required for All IP-Capable Nodes”, RFC 6540 / BCP 177, April 2012,
http://tools.ietf.org/html/bcp177

S. Farrell, H. Tschofenig, “Pervasive Monitoring Is an Attack”, RFC 7258 / BCP 188, May 2014,
http://tools.ietf.org/html/bcp188


R. Housley, “Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms”, RFC 7696 / BCP 201, November 2015,
http://tools.ietf.org/html/bcp201

W. Dennis, J. Bradley, “OAuth 2.0 for Native Apps”, RFC 8252 / BCP 212, October 2017,
http://tools.ietf.org/html/bcp212


T. Chown, J. Loughney, T. Winters, “IPv6 Node Requirements”, RFC 8504 / BCP 220, January 2019,

https://datatracker.ietf.org/doc/draft-ietf-tls-dtls13/

IPA, NIAP, and MFP Technical Community, “Protection Profile for Hardcopy Devices Version 1.0”, September 2015,

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity", IEEE 802.1AR-2018, June 2018,

IEEE, "IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks", IEEE 802.1AS-2011, February 2011,

IEEE, "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control", IEEE 802.1X-2010, February 2010,
https://standards.ieee.org/standard/802_1X-2010.html

IEEE, "IEEE Standard for Ethernet", IEEE 802.3-2018, August 2018,

IEEE, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE 802.11-2016, December 2016,
https://standards.ieee.org/standard/802_11-2016.html

IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE 802.11-2007, June 2007,

IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE 802.11-2012, March 2012,


1609.2-2016, January 2016, 
https://standards.ieee.org/standard/1609_2-2016.html

https://www.iso.org/standard/16387.html

https://www.iso.org/standard/45481.html

https://www.iso.org/standard/74528.html

https://www.iso.org/standard/69119.html

https://www.iso.org/standard/68564.html

https://www.iso.org/standard/52906.html

https://www.iso.org/standard/69466.html

https://www.itu.int/rec/T-REC-X.500

https://www.itu.int/rec/T-REC-X.509

https://www.itu.int/rec/T-REC-X.680

https://www.itu.int/rec/T-REC-X.690


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
</table>
602  [RFC2818] E. Rescorla. "HTTP Over TLS"
606  [RFC3022] P. Srisuresh, K. Egevang. "Traditional IP Network Address Translator (Traditional NAT)"
624  [RFC3629] T. Yergeau. "UTF-8, a transformation format of ISO 10646"


https://tools.ietf.org/html/rfc5424

<table>
<thead>
<tr>
<th>RFC</th>
<th>Reference</th>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
</table>


[RFC7472] I. McDonald, M. Sweet. "Internet Printing Protocol (IPP) over HTTPS Transport Binding and the 'ipps' URI Scheme"


[RFC7950] M. Bjorklund, “YANG 1.1 Data Modeling Language”, RFC 7950, August 2016,


11. Authors’ Addresses

Primary authors:

Ira McDonald
High North
PO Box 221
Grand Marais, MI 49839
blueroofmusic@gmail.com

The author would also like to thank the following individuals for their contributions to this white paper:

Brian Smithson (Ricoh)
Alan Sukert (Xerox)

12. Appendix A – Internet Protocol Suite

This section briefly summarizes selected protocols in the Internet Protocol Suite.

12.1 Internet Protocol Suite Evolution

The set of protocols in the Internet Suite (primarily defined by the IETF and IEEE) has evolved over fifty years based on changes in hardware and software architectures, network connectivity, reliability and security, and other functional requirements. An overview of the features and services of major Internet Suite protocols is included in [RFC8303].
12.2 Datalink Layer

12.2.1 ARP

Address Resolution Protocol (ARP) is defined in [RFC826]. ARP is a Datalink layer (OSI layer 2) protocol used in TCP/IP networks the Internet Protocol Suite. ARP supports mapping of one or more Network layer (OSI layer 3) IP addresses to their corresponding Datalink layer (OSI layer 2) hardware addresses (e.g., MAC addresses). ARP operates below the Network layer (OSI layer 3) as a part of the interface between the Network layer and Datalink layer.

12.2.2 DHCP

Dynamic Host Control Protocol (DHCP) is defined in [RFC2131]. DHCP is a Datalink layer (OSI layer 2) protocol used in TCP/IP networks the Internet Protocol Suite. DHCP supports network management of endpoints. A DHCP server can dynamically assign an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP operates below the Network layer (OSI layer 3) as a part of the interface between the Network layer and Datalink.

12.2.3 Ethernet

Ethernet is defined in [IEEE802.3]. Ethernet is a core Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. Ethernet supports sending and receiving Frames (i.e., Datalink Protocol Data Units (PDUs)) on wired Local Area Networks (LANs).

12.2.4 MACsec

MAC Security (MACsec) is defined in [IEEE802.1AE]. MACsec is a Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. MACsec supports data integrity and (optional) data encryption services for Ethernet or Wi-Fi endpoints participating in a MACsec security association.

12.2.5 MKA

MACsec Key Agreement (MKA) is defined in [IEEE802.1X]. MKA is a Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. MKA supports key management for establishment of security associations between Ethernet or Wi-Fi endpoints.

12.2.6 VLAN

Virtual LAN (VLAN) is defined in [IEEE802.1Q]. VLAN is a Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. VLANs support broadcast domains that are partitioned and logically isolated in a network at the Datalink layer (OSI layer 2) for Ethernet or Wi-Fi endpoints. VLAN tags are added and deleted by Ethernet or Wi-Fi Switches, transparently to the Ethernet or Wi-Fi endpoints.
12.2.7 Wi-Fi

Wi-Fi is defined in [IEEE802.11]. Wi-Fi is a core Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. Wi-Fi supports sending and receiving Frames (i.e., Datalink Protocol Data Units (PDUs)) on wireless Local Area Networks (LANs).

12.2.8 WPA2

Wi-Fi Protected Access II (WPA2™) is defined in [IEEE802.11i]. WPA2™ is a Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. WPA2™ supports data integrity and (optional) data encryption services for Wi-Fi endpoints participating in WPA2™ security associations.

The Wi-Fi Alliance introduced enhancements and new features in January 2018 for WPA2™ to ensure that WPA2™ maintains strong security protections as the wireless landscape evolves. WPA2™ continues to be mandatory for all Wi-Fi CERTIFIED devices.

12.2.9 WPA3

Wi-Fi Protected Access III (WPA3™) is defined by the Wi-Fi Alliance and was announced in June 2018. WPA3™ is a Datalink layer (OSI layer 2) protocol that can be used in TCP/IP networks the Internet Protocol Suite. WPA3™ supports data integrity and (optional) data encryption services for Wi-Fi endpoints participating in WPA3™ security associations.

WPA3™ introduces the next generation of Wi-Fi® security. WPA3™ supports new features to simplify Wi-Fi security, enable more robust authentication, and deliver increased cryptographic strength for highly sensitive data markets.

12.3 Network Layer

12.3.1 ICMP

Internet Control Message Protocol (ICMP) for IPv4 is defined in [RFC792]. ICMP is a Network layer (OSI layer 3) protocol used in TCP/IP networks the Internet Protocol Suite. ICMP supports network devices (e.g., Routers) sending error messages and operational information (e.g., a requested service is not available or a Host or Router could not be reached).

12.3.2 IP

Internet Protocol Version 4 (IPv4) is defined in [RFC791]. IP is the core Network layer (OSI layer 3) protocol used in TCP/IP networks the Internet Protocol Suite. IP supports sending and receiving network packets (i.e., Network Protocol Data Units (PDUs)). Due to IPv4’s limited address space (32-bit), IPv4 is slowly being supplanted by IP Version 6 (IPv6) defined in [RFC8200]. IPv6 includes a number of security enhancements over IPv4 and a much larger address space (128-bit).

12.3.3 IPsec

Internet Protocol Security (IPsec) is defined in [RFC4301]. IPsec is a secure Network layer (OSI layer 3) protocol used in TCP/IP networks the Internet Protocol Suite. IPsec supports network layer mutual authentication, data-origin authentication, data integrity, data confidentiality, etc.
IPsec uses cryptographic security services to protect communications between a pair of Hosts (Host-to-Host), a pair of Security Gateways (Network-to-Network), or a Security gateway and a Host (Network-to-Host).

12.3.4 NAT

Traditional Network Address Translation (NAT) for IPv4 is defined in [RFC3022]. NAT is a Network layer (OSI layer 3) protocol used in TCP/IP networks the Internet Protocol Suite. NAT supports remapping one IP address space into another IP address space by modifying network address information in the IP headers of Packets (i.e., Network Protocol Data Units (PDUs)) while they are in transit across a Router.

12.4 Transport Layer

12.4.1 TCP

Transmission Control Protocol (TCP) is defined in [RFC793]. TCP is the primary connection-oriented Transport layer (OSI layer 4) protocol used in TCP/IP networks the Internet Protocol Suite. TCP extensions and clarifications are summarized in the Roadmap to TCP [RFC7414]. TCP supports reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on endpoints in TCP/IP networks. TCP is used by major applications, such as the World Wide Web, email, remote administration, and file transfer.

12.4.2 TLS/DTLS

Transport Layer Security (TLS) Version 1.2 is defined in [RFC5246]. The successor TLS Version 1.3 is defined in [RFC8446]. TLS is the primary connection-oriented Transport layer (OSI layer 4) security protocol used above TCP the Internet Protocol Suite. Datagram Transport Layer Security (DTLS) Version 1.2 is defined in [RFC6347]. DTLS Version 1.3 is currently work-in-progress in [DTLS13]. DTLS is the primary connectionless Transport layer (OSI layer 4) security protocol used above UDP the Internet Protocol Suite. TLS and DTLS both provide equivalent data integrity (tamper protection) and data encryption (message confidentiality) services for end-to-end security associations. However, DTLS does not provide packet reordering services. TLS and DTLS share the same IANA TLS Registry of algorithms and parameters. TLS and DTLS both support single-sided authentication (server-only endpoint identity proof) and mutual authentication (client and server endpoint identity proofs).

TLS and DTLS security associations are created during the TLS Handshake phase when cipher suites are negotiated, single-sided or mutual authentication is performed, and shared secret symmetric keys are negotiated. TLS user data is transferred in the subsequent TLS Record phase. In each TLS version, the details of the TLS Handshake phase are different. Many TLS version-dependent standard extensions have been defined.

12.4.3 UDP

User Datagram Protocol (UDP) is defined in [RFC768]. UDP is the primary connectionless Transport layer (OSI layer 4) protocol used in TCP/IP networks the Internet Protocol Suite. Many
UDP standard extensions and clarifications are summarized in the Transport Features of UDP

[RFC8304]. UDP supports checksums for data integrity. UDP supports port numbers for addressing different functions at the source and destination of each datagram. UDP does not support a Handshake phase, and therefore it exposes application programs to any unreliability of the underlying network. UDP does not support any guarantee of delivery, ordering, or duplicate detection.

### 12.5 Session Layer

#### 12.5.1 ICE

Interactive Connectivity Establishment (ICE) is defined in [RFC5245]. ICE is a Session layer (OSI layer 5) protocol used in TCP/IP networks the Internet Protocol Suite. ICE uses STUN and its extension TURN. ICE can be used by any protocol utilizing the offer/answer model, such as the Session Initiation Protocol (SIP).

#### 12.5.2 HTTP

Hypertext Transfer Protocol (HTTP) Version 1.1 is defined in [RFC7230]. HTTP Version 2 is defined in [RFC7540]. HTTP is a Session layer (OSI layer 5) protocol used in TCP/IP networks the Internet Protocol Suite. HTTP is also often used to support Application layer (OSI layer 7) protocols, for example, the Internet Printing Protocol defined in [STD92]. This use of HTTP as a substrate is defined in [RFC3205] / [BCP56].

#### 12.5.3 STUN

Session Traversal Utilities for NAT (STUN) is defined in [RFC5389]. STUN is a Session layer (OSI layer 5) protocol used in TCP/IP networks the Internet Protocol Suite. STUN supports the detection and traversal of NATs or Firewalls that are located in the communications paths between endpoints. STUN is a lightweight Client-Server protocol, requiring only simple query and response components with a third-party Server located on a common, easily accessible network, typically the public Internet. STUN messages are sent in UDP, DTLS, TCP, or TLS packets.

#### 12.5.4 TURN

Traversal Using Relays around NAT (TURN) for IPv4 is defined in [RFC5766]. TURN for IPv6 is defined in (RFC6156). TURN is a Session layer (OSI layer 5) protocol used in TCP/IP networks the Internet Protocol Suite. TURN supports the detection and traversal of NATs or Firewalls that are located in the communications paths between endpoints. TURN messages are sent in UDP, DTLS, TCP, or TLS packets.

### 12.6 Presentation Layer

The Internet Protocol Suite does include Presentation layer (OSI layer 6) data encoding protocols. However, these protocols are always embedded in specific Application layer (OSI layer 7) protocols, often without version negotiation.
12.6.1 ASN.1

Abstract Syntax Notation One (ASN.1) is defined in [ITU-X.680]. ASN.1 is a Presentation layer (OSI layer 6) protocol that can be used in TCP/IP networks the Internet Protocol Suite. ASN.1 is an interface description language (IDL) for defining data structures that can be serialized in standard, cross-platform forms.

ASN.1 is widely used in telecommunications and computer networking, and especially in cryptography. For example, the SNMP MIB definition languages SMIV1 and SMIV2 are defined in ASN.1. Public Key Infrastructure (PKI) interfaces such as [ITU-X.509] certificates are defined in ASN.1. LDAP directory schema are defined in ASN.1. Several standard encoding schemes are defined for ASN.1 including: Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER), all of which are defined in [ITU-X.690]; Packed Encoding Rules (PER) defined in [ITU-X.691]; and XML Encoding Rules (XER) defined in [ITU-X.693].

12.6.2 CBOR

Concise Binary Object Representation (CBOR) is defined in [RFC7049] in the Internet Protocol Suite. CBOR is a lightweight, binary, data interchange format whose design goals include extremely small code size, fairly small message size, and extensibility without version negotiation. These design goals make CBOR fundamentally different from earlier binary serializations such as ASN.1. CBOR datatypes are a superset of JSON (RFC8259) datatypes. CBOR is widely used in IETF, ISO, ITU-T, and telecom industry specifications and protocols.

12.6.3 CDDL

Concise Data Definition Language (CDDL) is defined in [RFC8610] in the Internet Protocol Suite. CDDL is the only IETF standards-track schema language that can express both CBOR [RFC7049] and JSON [RFC8259] data structures. CDDL is widely used in IETF, ISO, ITU-T, and telecom industry specifications and protocols.

12.6.4 HTML

Hypertext Markup Language (HTML) Version 2.0 is defined in [RFC1866]. HTML Version 4.0 is defined in [RFC2854]. HTML in the Internet Protocol Suite has been in use as a markup language for web pages in the World Wide Web information infrastructure since 1990. HTML was extended by the World Wide Web Consortium (W3C) in v3.2 (1997), v4.0 (1998), and v4.01 (1999). HTML v5.2 [HTML5.2] was defined by the W3C in 2017.

12.6.5 JSON

JavaScript Object Notation (JSON) is defined in [RFC8259] in the Internet Protocol Suite. JSON is a lightweight, text-based, data interchange format. JSON was derived from the ECMAScript Programming Language Standard. JSON defines a small set of formatting rules for the portable representation of structured data. See CBOR above.
12.6.6 REST

Representational State Transfer (REST) was originally described in Roy Fielding’s doctoral dissertation in 2000. REST is an architectural style that defines a set of constraints that can be used for creating web services in the Internet Protocol Suite. REST-based web services allow the requesting systems to access and manipulate textual representations of web resources by using a uniform and predefined set of stateless operations. The IETF does NOT recognize any normative definition of the REST architectural style. The RESTCONF protocol is defined in [RFC8040]. RESTCONF transfers data defined in YANG schema [RFC7950] over HTTP and was derived from the original NETCONF protocol defined in [RFC6241]. The IETF chartered the CORE WG (Constrained RESTful Environments) which has published a number of Internet standards-track RFCs for the Internet-of-Things (IoT) market.

12.6.7 SGML

Standard Generalized Markup Language (SGML) is defined in [ISO8879]. SGML can be used in the Internet Protocol Suite for defining generalized markup languages for documents. SGML is based on two postulates: (a) markup should be declarative; and (b) markup should be rigorous.

HTML was theoretically an example of an SGML-based language until HTML 5, which browsers cannot parse as SGML for compatibility reasons.

12.6.8 Unicode

Unicode Version 12.1 [Unicode] was defined by the Unicode Consortium in May 2019 that can be used in the Internet Protocol Suite. Unicode is the primary international standard for the consistent encoding, representation, and handling of text expressed in most of the world’s writing systems. Unicode 12.1 contains a repertoire of 137,929 characters covering 146 modern and historic scripts, as well as multiple symbol sets and emoji. The character repertoire of the Unicode Standard is synchronized with [ISO10646] and the assigned codepoints in both standards are identical.

12.6.9 UTF-8

UTF-8 is a serialization (transformation format) of Unicode [Unicode] that can be used in the Internet Protocol Suite. UTF-8 is defined by the Unicode Consortium and is described in [RFC3629]. Network Unicode is defined in [RFC5198] as a constrained format of UTF-8 with mandatory normalization and specific line ending sequences for internationalized text exchange on the Internet. UTF-8 is supported in all IETF standards-track protocols and is now the mandatory default character set in most IETF standards-track protocols.

12.6.10 UTF-16

UTF-16 is an obsolete serialization (transformation format) of Unicode [Unicode] that was used in the Internet Protocol Suite.

Note: UTF-16 is now obsolete and is unsuitable for use in any network protocol.
12.6.11 UTF-32

UTF-32 is an obsolete serialization (transformation format) of Unicode [Unicode] that was used in the Internet Protocol Suite.

Note: UTF-32 is now obsolete and is unsuitable for use in any network protocol.

12.6.12 XML

Extensible Markup Language (XML) is defined by the World Wide Web Consortium (W3C) in [XML][W3C-XML] that can be used in the Internet Protocol Suite. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

The design goals of XML emphasize simplicity, generality, and usability across the Internet. XML is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, the language is widely used for the representation of arbitrary data structures such as those used in Web Services.

12.6.13 XSD

XML Schema Definition (XSD) is defined by the World Wide Web Consortium (W3C) in [XSD][W3C-XSD] that can be used in the Internet Protocol Suite. XSD can be used to express a set of rules to which an XML document must conform in order to be considered "valid" according to a given schema. XSD was also designed with the intent that determination of a document's validity would produce a collection of information adhering to specific data types.

12.6.14 YANG

YANG is defined in [RFC7950] and updated in [RFC8342] and [RFC8526]. YANG is a data modeling language (i.e., schema language) in the Internet Protocol Suite. YANG was originally designed to model configuration and state data that can be modified with the Network Configuration Protocol (NETCONF) [RFC6241], NETCONF Remote Procedure Calls, and NETCONF notifications. YANG has now been used as a schema language for many other IETF standards-track other protocols, such as RESTCONF [RFC8040].

12.7 Application Layer

12.7.1 DNS

Domain Name System (DNS) is defined in [RFC1035] in the Internet Protocol Suite. DNS is a hierarchical, decentralized, naming system for computers, services, and other resources connected to the Internet or any private network that uses the Internet Protocol Suite. DNS maps domain names, assigned to each of the participating entities, to Network layer (OSI layer 3) IP addresses. Network administrators can delegate authority over sub-domains of their allocated name space to other name servers.

Commented [IM3]: Add “RADIUS/DIAMETER” and “OAUTH2” and “KERBEROS” sections for authentication and authorization services.
12.7.2 FTP

File Transfer Protocol (FTP) is defined in [RFC959] in the Internet Protocol Suite. FTP is the primary file transfer protocol in the Internet Protocol Suite. FTP is used to transfer files between clients and servers on the Internet or any private network that uses the Internet Protocol Suite. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users can authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password. FTP users can also connect anonymously, if the FTP server is configured to allow it.

FTPS is defined in [RFC4217] in the Internet Protocol Suite. FTPS consists of FTP over TLS. FTPS supports secure file transmission that protects the username and password (or other authentication credentials) and supports content encryption.

Note: SFTP has never been standardized in the Internet Protocol Suite. SFTP consists of FTP over Secure Shell (SSH) [RFC4253]. Six versions of SFTP that are not interoperable have all failed to ever reach Internet standard publication over the past 20 years. Therefore, SFTP is unsuitable for use in any HCD.

12.7.3 HTTP

Hypertext Transfer Protocol (HTTP) Version 1.1 is defined in [RFC7230] in the Internet Protocol Suite. HTTP supports distributed, collaborative, and hypermedia information systems. HTTP is the primary data communication protocol for the World Wide Web.

HTTPS is defined in [RFC2818] in the Internet Protocol Suite. HTTPS consists of HTTP/1.1 over TLS. HTTPS supports secure message transmission that protects the username and password (or other authentication credentials) and supports content encryption.

HTTP Version 2 is defined in [RFC7540] in the Internet Protocol Suite. HTTP/2.0 enables a more efficient use of network resources. HTTP/2.0 is intended to reduce user latency perception, by introducing header field compression and allowing multiple concurrent exchanges on the same connection. HTTP/2.0 also introduces unsolicited push of messages from servers to clients. HTTP/2.0 does not obsolete HTTP/1.1. Underlying HTTP operation semantics remain unchanged.

12.7.4 IMAP

Internet Message Access Protocol (IMAP) Version 4 is defined in [RFC3501] in the Internet Protocol Suite. IMAP is used by email clients to retrieve email messages from a mail server over a TCP/IP connection.

IMAPS is defined in [RFC2595] in the Internet Protocol Suite. IMAPS consists of IMAP over TLS. IMAPS supports secure email transmission that protects the username and password (or other authentication credentials) and supports content encryption.

12.7.5 IPP

Internet Printing Protocol (IPP) Version 1.1 is defined in [STD92] in the Internet Protocol Suite. IPP supports distributed printing using Internet tools and technologies. [RFC8011] defines a simplified model consisting of abstract objects, attributes, and operations that is independent of the wire
encoding and transport protocols. [RFC8010] defines a concrete binding of the IPP abstract model onto HTTP and TLS.

The ‘ipp’ URI scheme is defined in [RFC3510]. The ‘ipps’ URI scheme is defined in [RFC7472].

12.7.6 LDAP


12.7.7 MQTT

Message Queuing Telemetry Transport (MQTT) v3.1.1 is defined in [ISO20922] that can be used in the Internet Protocol Suite. MQTT is a publish/subscribe messaging transport protocol that is designed to be open and lightweight. MQTT is designed for constrained environments, where a small code footprint and/or minimum network bandwidth is required. MQTT can be run over TCP/IP or other network protocols that provide ordered, lossless, bi-directional connections. MQTT over TLS can be used for secure message transmission that protects the username and password (or other authentication credentials) and supports content encryption.

Note: MQTT without TLS is inherently dangerous. Therefore, MQTT without TLS with mutual authentication is unsuitable for use in any HCD.

12.7.8 NETCONF

Network Configuration Protocol (NETCONF) is defined in [RFC6241] in the Internet Protocol Suite. NETCONF is a publish/subscribe network management protocol. NETCONF supports mechanisms to install, modify, and delete the configuration of network devices. NETCONF uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages. NETCONF protocol operations are defined as remote procedure calls (RPCs).

12.7.9 NTP

Network Time Protocol (NTP) Version 4 is defined in [RFC5905] in the Internet Protocol Suite. NTP Autokey (for security) is defined in [RFC5906], but not widely deployed. NTP supports clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP endpoints can usually tens of milliseconds accuracy over the public Internet.

Security requirements for NTP and Precision Time Protocol (PTP) are defined in [RFC7384]. IETF NTP security extensions are currently work-in-progress in Network Time Service for NTP [NTSNTP].

12.7.10 POP

Post Office Protocol (POP) Version 3 is defined in [RFC1939] in the Internet Protocol Suite. POP is used by email clients to retrieve email messages from a mail server over a TCP/IP connection.
Most POP clients have an option to leave the mail on the server after download. However, most POP clients usually retrieve all messages, store them on the client system, and delete them from the server. POP has been superseded by IMAP.

POPS is defined in [RFC2595] in the Internet Protocol Suite, and POPS consists of POP over TLS. POPS supports secure email transmission that protects the username and password (or other authentication credentials) and provides content encryption.

12.7.11 RESTCONF

RESTCONF is defined in [RFC8040] in the Internet Protocol Suite. RESTCONF is a publish/subscribe network management protocol. RESTCONF is an HTTP-based protocol that supports a programmatic interface for accessing data defined in YANG [RFC7950], using the datastore concepts defined in NETCONF [RFC6241].

12.7.12 SIP

Session Initiation Protocol (SIP) is defined in [RFC3261] in the Internet Protocol Suite. SIP is used for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, as well as in instant messaging over Internet Protocol (IP) networks. SIP can run over UDP, TCP, or SCTP. For transmission of media streams (voice, video) SIP typically employs either Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP).

The 'sips' URI scheme is defined in [RFC5630] for running SIP over TLS.

12.7.13 SMIv1

Structure of Management Information Version 1 (SMIv1) is obsolete and is defined in [RFC1155], [RFC1212], and [RFC1215] in the Internet Protocol Suite used to define SNMP MIBs and specified in ASN.1 [ITU-X.680].

12.7.14 SMIv2

SMI Version 2 (SMIv2) is an Internet Standard defined in [RFC2578], [RFC2579], and [RFC2580] in the Internet Protocol Suite used to define SNMP MIBs and specified in ASN.1 [ITU-X.680].

12.7.15 SMTP

Simple Mail Transfer Protocol (SMTP) is defined in [RFC5321] in the Internet Protocol Suite. SMTP supports sending and receiving email messages between mail clients, mail servers, and mail transfer agents (MTAs).

SMTP is defined in [RFC3207] in the Internet Protocol Suite, and SMTPS consists of SMTP over TLS. SMTPS supports secure email transmission that protects the username and password (or other authentication credentials) and provides content encryption.
12.7.14 Simple Network Management Protocol (SNMP) Version 1 is obsolete and is defined in [RFC1157] in the Internet Protocol Suite. SNMPv1 protocol is obsolete. SNMP Version 2 is obsolete and is defined in [RFC3416] and [RFC3417] in the Internet Protocol Suite. SNMPv2 protocol is also obsolete.

SNMP Version 3 is an Internet Standard defined in [RFC3410] through [RFC3417] in the Internet Protocol Suite. Coexistence between SNMPv1, SNMPv2, and SNMPv3 (but with very little security) is defined in [RFC3584].

SNMP supports collecting information about managed devices on Internet Protocol Suite TCP/IP networks. SNMP also supports modifying that information to change device behavior. SNMP is ubiquitous. SNMP is the most widely network management protocol in existence. SNMP Agents (on managed devices) expose management data organized into management information bases (MIBs). MIBs describe system status and configuration. SNMP support is mandatory for all intermediate network devices (e.g., Routers) that are connected to the public Internet.

SNMP MIBs are device management models written in either: (a) the obsolete Structure of Management Information Version 1 ([SMIV1]) defined in [RFC1155], [RFC1212], and [RFC1215]; or (b) the Internet Standard SMI Version 2 ([SMIV2]) defined in [RFC2578], [RFC2579], and [RFC2580]. SMIV1 and SMIV2 are both management schema languages specified in ASN.1 [ITU-X.680].

SNMPv3 over TLS is defined in [RFC5590], [RFC5591], and [RFC5593] in. SNMPv3 over TLS supports secure SNMP message transmission that protects the username and password (or other authentication credentials) and provides content encryption.

12.7.15 SSH

Secure Shell (SSH) is defined in [RFC4253] and [RFC4254] in the Internet Protocol Suite. SSH is primarily used for secure remote command-line login and secure remote command execution. SSH can also be used to secure other remote services.

Note: SSH is inherently dangerous, because implementation or configuration errors can allow privilege escalation and unconstrained remote shell capabilities on target systems. SSH has major security flaws and has often been used for widespread Internet attacks by intelligence agencies and criminal organizations. Therefore, SSH is unsuitable for use in any HCD.

12.7.16 Syslog

Syslog is defined in [RFC5424] in the Internet Protocol Suite. Syslog is used to store event notification messages in a network Audit Log. The Syslog protocol utilizes a layered architecture, which allows the use of any number of transport protocols for transmission of Syslog messages. It also provides a message format that allows vendor-specific extensions to be provided in a structured way. Syslog is the primary Audit Log technology used in all modern operating systems.

Syslog over TLS is defined in [RFC5425] in the Internet Protocol Suite. Syslog over TLS supports secure connections for the transport of Syslog messages. [RFC5425] describes the security threats to Syslog and how TLS can be used to counter such threats.
Telnet is defined in [RFC854] in the Internet Protocol Suite. Historically, Telnet was used to provide access to command-line interfaces on remote systems, including most network equipment and operating systems with any configuration utility.

Note: Telnet is inherently dangerous, because it always passes user name, user password, and user commands in cleartext. Therefore, Telnet is unsuitable for use in any HCD.

13. Change History

13.1 20 January 2020

Interim draft – updates from IDS WG review on 9 January 2020.
- Corrected author and title metadata.
- Corrected title of HCDPP in section 1 Introduction and section 10 References (need URI).
- Revised section 2.3 Security Terminology to delete trailing “d” and at end of section.
- Revised section 3.4 Design Requirements to change “5100.4” to “5110.4” and correct spelling of recommendations.
- Revised section 6. HCD System Architecture to change “channel” to “channel isolation”.
- Revised section 10. References to delete leading space in [BCP61], change [XML] to [W3C-XML], change [XSD] to [W3C-XSD], and fix broken format of [W3C-XSD].
- Revised section 12 Appendix A – Internet Protocol Suite to distinguish which protocols “can be used in the Internet Protocol Suite” (non-IETF protocols) from protocols “in the Internet Protocol Suite” (IETF protocols) and also to change “is is” to “is” in Syslog subsection.
- TODO – Move all notes on inappropriate protocols for HCDs from section 12 to section 4 (when those subsections are added).

13.2 31 December 2019

Interim draft – updates from discussions at PWG Virtual F2F meetings in August 2019 and November 2019.
- Revised document class and filename from White Paper to IDS Best Practice per IDS WG discussion.
- Revised section 3 Requirements to add use cases from [PWG5110.1], exceptions, out-of-scope requirements, and design requirements.
- Revised section 4 HCD Network Security, section 5 HCD Local Security, and section 6 HCD System Architecture to add primary subsections and comments about intended contents.
- Revised section 10 References to add many references.
- Added section 12 Appendix A – Internet Protocol Suite.

**11 July 2019**

Interim draft – additional content after PWG Virtual F2F in February 2019.

- Revised section 3.1 Rationale to change “host-based” to “local” for the HCD’s own firewalls, IDS systems, etc. (as opposed to perimeter security in other network intermediate systems), per Cihan Colakoglu.
- Added titles and brief descriptions for section 4 HCD Network Security, section 5 HCD Local Security, section 6 HCD System Architecture, and section 7 Conformance, to clarify the intended scope and structure of this document.

**13 February 2019**

Initial revision.