IHE Change Proposal

Tracking information

IHE Domain:	IT Infrastructure
Change Proposal ID:	CP-ITI-1332
Change Proposal Status:	Submitted
Date of last update:	9 June 2026
Person assigned:	Steve Nichols

Change Proposal Summary Information

Update RFC references in ATNA	
Submitter's Name(s) and email address(es):	steven.nichols@gehealthcare.com
Submission Date:	16 April 2026
Profile(s) affected:	ATNA
Actor(s) affected:	All
IHE Technical Framework or Supplement modified:	ITI TF-1 ITI TF-2
Volume(s) and Section(s) affected:	ITI TF-1: 9.2 ITI TF-2: 3.20

Detailed Rationale for Change:

The current IHE ATNA specification references RFC 5425 (Transmission of Syslog Messages over TLS) as the required transport mechanism for audit messages.

RFC 9662 updated cipher suites required by RFC 5425. However, replacing RFC5425 outright would constitute a breaking change and invalidate a large installed base of systems currently conformant to ATNA and SYSLOG-TLS.

In parallel, DICOM is progressing a corresponding Change Proposal to similarly allow the use of RFC 5425 or RFC 9662 for audit message transport.

This CP also removes an obsolete DICOM reference and correct minor type-os and formatting.

Note: ASTM E2147 has recently been transferred to HL7, where it is expected to be maintained and evolved within the HL7 standards framework. This transition does not immediately change the semantics of ATNA audit requirements but may enable future alignment with HL7-based audit representations.

Notes 9 June 2026 CP call:
ATX: TLS Syslog Option

The existing **ATX: TLS Syslog Option** permits use of Syslog over TLS but does not constrain the negotiated TLS version. As a result, it may allow deprecated TLS versions such as TLS 1.0 or TLS 1.1, depending on implementation and configuration.

Potential approaches:

1. **Keep the option unchanged**
    - Preserves backward compatibility.
    - Avoids invalidating existing Integration Statements.
    - This is the current approach in CP-ITI-1332.
2. **Update the option to prohibit TLS 1.0 and TLS 1.1**
    - Aligns the option with current TLS security expectations.
    - Introduces a breaking change for existing implementations that rely on the current option behavior.

3. **Retire the option**
    - Removes ambiguity around use of deprecated TLS versions.
    - Would require clear migration guidance, likely toward a newer ATX option with explicit TLS version and cipher-suite requirements.

Matt will check with Lynn and Steve Moore on the recommended approach.

Related Question: STX: TLS 1.2 Floor using BCP195 Option

This discussion also raises the question of whether the existing **STX: TLS 1.2 Floor using BCP195 Option** should be retired or revised.

The option was intended to let products claim conformance to current TLS best practice as **BCP 195** evolved, without creating a new option each time the underlying IETF guidance changed. However, this creates ambiguity for Integration Statements because products do not automatically update when BCP 195 changes. Customers reviewing Integration Statements must infer which RFC baseline applied when the statement was created.

A more testable approach would be to define options using specific RFC baselines and explicit TLS/cipher-suite requirements, rather than relying on a moving BCP reference.

Proposed Change(s)

Update Vol1, Table 9.2-1 as follows:

Table 9.2-1: ATNA - Actors and Options

Actor	Options	Vol. & Section
Audit Record Repository (Note 4)	**ATX: TLS 1.2 Floor using RFC 9662**	**ITI TF-1: 9.2.7.4**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Audit Record Forwarder (Note 4)	**ATX: TLS 1.2 Floor using RFC 9662**	**ITI TF-1: 9.2.7.4**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Secure Node (Note 1) (Note 4)	Radiology Audit Trail	ITI TF-1: 9.2.2 RAD TF-3: 5.1
	FQDN Validation of Server Certificate (Note 2)	ITI TF-1: 9.2.5 ITI TF-2: 3.19.6.1.4
	STX: No Secure Transport	ITI TF-1: 9.2.6.1
	STX: TLS 1.2 Floor using BCP195	ITI TF-1: 9.2.6.4
	STX: S/MIME	ITI TF-1: 9.2.6.5
	STX: WS-Security	ITI TF-1: 9.2.6.6

Actor	Options	Vol. & Section
	ATX: TLS 1.2 Floor using RFC 9662	**ITI TF-1: 9.2.7.4**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Secure Application (Note 1) (Note 4)	Radiology Audit Trail	ITI TF-1: 9.2.2 RAD TF-3: 5.1
	FQDN Validation of Server Certificate (Note 2)	ITI TF-1: 9.2.5 ITI TF-2: 3.19.6.1.4
	STX: No Secure Transport	ITI TF-1: 9.2.6.1
	STX: TLS 1.2 Floor using BCP195	ITI TF-1: 9.2.6.4
	STX: S/MIME	ITI TF-1: 9.2.6.5
	STX: WS-Security	ITI TF-1: 9.2.6.6
	ATX: TLS 1.2 Floor using RFC 9662	**ITI TF-1: 9.2.7.4**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3

Note 1: *Secure Node and Secure Application shall support at least one of the "STX" (Secure Transport) options.*

Note 2: *The "FQDN Validation of Server Certificate" Option is only applicable to TLS-based Secure Transports.*

Note 3: *Intentionally left blank.*

Note 4: *This actor shall support at least one of the "ATX" (Audit Transport) options. If a product's IHE Integration Statement does not declare one of these options, the reader should assume that the product supports the TLS or UDP Syslog Option.*

Update Vol2, 9.2.6.4 STX: TLS 1.2 Floor using BCP195 Option as follows:

9.2.6.4 STX: TLS 1.2 Floor using BCP195 Option

Actors that support this option have the ability to both:

- Operate with the highest level of cyber protection for the TLS-protected communication channel per the IETF Best Current Practice (BCP195 **[RFC9325]** with TLS 1.2 and selected cipher suites), and
- Restrict to the use of TLS version 1.2 [RFC5246] or higher.

This option adopts valuable recommendations from the IETF BCP195 and prohibits less secure behavior. It is well suited for ensuring a high level of cyber protection.

~~Note: The STX: TLS 1.2 Floor using BCP195 Option is equivalent to the DICOM "Non-Downgrading BCP 195 TLS Secure Transport Connection Profile". See DICOM PS3.15 Section B.10.~~

Note: TLS version 1.3 [RFC8446] may be used where supported.

An actor that supports the STX: TLS 1.2 Floor using BCP195 Option shall be able to comply with BCP195 **[RFC9325]** with the additional restrictions enumerated in ITI TF-2: 3.19.6.2.3 .

Add Vol1, 9.2.7.4 ATX: TLS 1.2 Floor using RFC 9662 Option as follows:

9.2.7.4 ATX: TLS 1.2 Floor using RFC 9662 Option

Actors that support this option have the ability to both:

- Operate with a high level of cyber protection for the TLS-protected Syslog communication channel in accordance with the IETF Best Current Practice (BCP 195, [RFC9325] as updated by [RFC9662]), and
- Restrict the use of TLS to version 1.2 [RFC5246] or higher.

This option adopts current recommendations from the IETF BCP 195, including updates from RFC 9662, and prohibits less secure behavior. It is well suited for ensuring a high level of cyber protection for audit log transport using Syslog over TLS.

Note: TLS version 1.3 [RFC8446] may be used where supported.

An actor that supports the ATX: TLS 1.2 Floor using RFC 9662 Option shall be able to comply with BCP 195 [RFC9325] as updated by [RFC 9662] when using TLS for Syslog transport as defined in the Record Audit Event [ITI-20] transaction.

Update Vol2, Section 3.20.3 as follows:

3.20.3 Referenced Standards

RFC5424	The Syslog Protocol.
RFC5425	Transmission of Syslog Messages over TLS
RFC5426	Transmission of Syslog Messages over UDP
RFC7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
RFC 8446	**The Transport Layer Security (TLS) Protocol Version 1.3**
RFC 9325	**Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**
RFC 9662	**Updates to the Cipher Suites in Secure Syslog**
DICOM	DICOM PS3.15 Annex A.5 http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html
ASTM E2147-01	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
NIST SP 800-92	Guide to Computer Security Log Management.
W3C XML 1.0	Extensible Markup Language (XML) 1.0

Update Section 3.20.4.1.2.1 as follows:

3.20.4.1.2.1 Audit Message Transports

This transaction defines two transport mechanisms for Record Audit Event messages:

1. Transmission of Syslog messages over TLS (RFC_5425) with ~~**The**~~ **the** Syslog Protocol (RFC 5424) which formalizes sending Syslog messages over a streaming protocol protectable by TLS. See Section 3.20.4.1.2.1.1.
2. Transmission of Syslog messages over UDP (RFC_5426) with The Syslog Protocol (RFC_5424) which formalizes and obsoletes BSD Syslog protocol defined in RFC_3164. See Section 3.20.4.1.2.1.2.

3.20.4.1.2.1.1 Transmission of Syslog Messages over TLS

Transmission of Syslog messages over TLS (RFC 5425) with the Syslog Protocol (RFC 5424) formalizes sending Syslog messages over a streaming protocol ~~**protectable**~~ **protected** by TLS.

RFC 5425 requires the use of TLS for transport but does not mandate a specific TLS version. When the ATNA ATX: TLS 1.2 Floor using RFC 9662 Option is declared, TLS version 1.2 or higher shall be used in accordance with this option.

~~**RFC5424 states that this MUST be TLS version 1.2. For this transaction, that requirement is relaxed to be that it MUST be TLS; version 1.2 is RECOMMENDED.**~~