DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2020/01/17
Person Assigned	Rob Horn
Submitter Name	Rob Horn
Submission Date	2019/05/29

Correction Number CP- 1947
Log Summary: Add security considerations for encapsulated formats
Name of Standard PS3.3, PS3.5 2019e
Rationale for Correction: DICOM encapsulates externally designed information formats such as JPEG and PDF in a variety of ways. These formats have had security issues, both with the format itself and with common implementations for processing the format. This adds a security considerations section near the text that includes the reference to the encapsulated format, to alert the reader to the need to check elsewhere for any additional security considerations related to the encapsulated format.
Correction Wording:

Add section C.24.2.3 to Encapsulated Document Module

This covers the PDF, 3D Manufacturing, and other encapsulated IODs.

C.24.2.3 Security Considerations for Encapsulated Documents (Informative)

The encapsulated documents may conform to another standard, e.g., PDF, or may be in a proprietary format. Many of these formats have had their own security issues, both with the format itself and with common implementations for processing the format.

Implementations that support encapsulated documents may need to:

- Perform input validation and sanitation to detect and perhaps remove invalid or malicious content.
- Perform output validation to ensure safe compliance with format specification.
- Monitor library implementations for vulnerability reports, updates, and have a process for managing these updates.

Tracking, notification, and remediation of these security problems will normally be in the context of the encapsulated format and not in the context of DICOM. This means those implementing and deploying the encapsulated format must consider security issues from those other contexts.

Add section 8.5 to PS 3.5 Data Structures and Encoding

This covers the JPEG, MPEG, and other encapsulated formats for Pixel, Overlay, and Waveform data.

8.5 SECURITY CONSIDERATIONS FOR ENCODING OF PIXEL, OVERLAY, AND WAVEFORM DATA (INFORMATIVE)

The encapsulated formats conform to other standards, e.g., JPEG. Many of these formats have had their own security issues, both with the format itself and with common implementations for processing the format.

Implementations that support encapsulated format encoding may need to:

- Perform input validation and sanitation to detect and perhaps remove invalid or malicious content.
- Perform output validation to ensure safe compliance with format specification.
- Monitor library implementations for vulnerability reports, updates, and have a process for managing these updates.

Tracking, notification, and remediation of these security problems will normally be in the context of the encapsulated format and not in the context of DICOM. This means those implementing and deploying the encapsulated format must consider security issues from those other contexts.