Guide to Schemas for DHZM

DHZM Schema Guide

Version 2021-JAN

January 15, 2021

Table of Contents

Chapter 1 - Introduction

1.1 - Purpose

This is an informative supplement for DHZM. This guide is generated from the DHZM Schemas and provides a consolidated reference for the schemas of this specification.

Chapter 2 - Schema Files

2.1 - DHZM.xsd

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns="urn:us:gov:ic:digitalhazmat"
                        xmlns:xhtml="http://www.w3.org/1999/xhtml-StopBrowserRendering"
                        xmlns:dhzm="urn:us:gov:ic:digitalhazmat"
                        xmlns:tdf="urn:us:gov:ic:tdf"
                        xmlns:icsfhashv="urn:us:gov:ic:sf:hashverification"
                        xmlns:icsf="urn:us:gov:ic:sf"
                        targetNamespace="urn:us:gov:ic:digitalhazmat"
                        elementFormDefault="qualified"
                        attributeFormDefault="qualified"
                        ism:DESVersion="201903.202010"
                        ism:ISMCATCESVersion="202010"
                        ism:compliesWith="USGov USIC"
                        ism:createDate="2019-09-18"
                        ism:resourceElement="true"
                        ism:classification="U"
                        ism:ownerProducer="USA"
                        version="202101">
                <xs:import namespace="urn:us:gov:ic:sf:hashverification"
                           schemaLocation="../IC-SF/HashVerification.xsd"/>
                <xs:import namespace="urn:us:gov:ic:sf" schemaLocation="../IC-SF/IC-SF.xsd"/>
                <xs:annotation>
                    <xs:documentation>
                              <xhtml:h1 ism:ownerProducer="USA" ism:classification="U">Intelligence Community Technical Specification XML Data
                                        Encoding Specification for DigitalHazMat Assertion
                                        (DHZM.XML)</xhtml:h1>
                    </xs:documentation>
                    <xs:documentation>
                              <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Notices</xhtml:h2>
                              <xhtml:p ism:ownerProducer="USA" ism:classification="U">Distribution Notice:
    This document has been approved for Public Release and is available for use without restriction.
</xhtml:p>
                    </xs:documentation>
                    <xs:documentation>
                              <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Description</xhtml:h2>
                              <xhtml:p ism:ownerProducer="USA" ism:classification="U">W3C XML
                                        Schema for the XML Data Encoding Specification for XML Data
                                        Encoding Specification for DigitalHazMat Assertion
                                        (DHZM.XML).</xhtml:p>
                    </xs:documentation>
                    <xs:documentation>
                              <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Introduction</xhtml:h2>
                              <xhtml:p ism:ownerProducer="USA" ism:classification="U">This XML
                                        Schema file is one component of the XML Data Encoding
                                        Specification (DES). Please see the document titled<xhtml:i>
                                              <xhtml:a href="../../Documents/DHZM/DesDhzmXml.pdf">XML
                                                        Data Encoding Specification for DigitalHazMat Assertion</xhtml:a>
                                        </xhtml:i>for a complete description of the encoding as
                                        well as list of all components.</xhtml:p>
```

```
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">It is
                    envisioned that this schema or its components, as well
                    as other parts of the DES may be overridden for
                    localized implementations. Therefore, permission to use,
                    copy, modify and distribute this XML Schema and the
                    other parts of the DES for any purpose is hereby granted
                    in perpetuity.</xhtml:p>
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Please
                    reference the preceding two paragraphs in all copies or
                    variations. The developers make no representation about
                    the suitability of the schema or DES for any purpose. It
                    is provided "as is" without expressed or implied
                    warranty.</xhtml:p>
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">If you
                    modify this XML Schema in any way label your schema as a
                    variant of DHZM.XML.</xhtml:p>
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Please
                    direct all questions, bug reports,or suggestions for
                    changes to the points of contact identified in the
                    document referenced above.</xhtml:p>
            </xs:documentation>
            <xs:documentation>
                <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Implementation Notes</xhtml:h2>
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">The root elements for DigitalHazMat Assertions
                    can be either <xhtml:a href="DHZM_xsd_Element_ProvenanceAssertion.html#ProvenanceAssertion">dhzm:ProvenanceAssertion</xhtml:a>
                    or <xhtml:a href="DHZM_xsd_Element_AnalysisAssertion.html#AnalysisAssertion">dhzm:AnalysisAssertion</xhtml:a>
                    and are implemented as a TDF assertions.
                </xhtml:p>
            </xs:documentation>
            <xs:documentation>
                <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Creators</xhtml:h2>
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Office of
                    the Director of National Intelligence Intelligence
                    Community Chief Information Officer</xhtml:p>
            </xs:documentation>
        </xs:annotation>

        <!--*************************************************-->

<!-- Start Elements                                  -->

<!--*************************************************-->


<!-- Root Element -->

<xs:element name="ProvenanceAssertion" type="dhzm:ProvenanceAssertionType">
            <xs:annotation>
                <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">The root node of a provenance assertion for cross domain transfer.</xhtml:p>
                </xs:documentation>
            </xs:annotation>
        </xs:element>
```

```
        <!-- Root Element -->

    <xs:element name="AnalysisAssertion" type="dhzm:AnalysisAssertionType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">The root node of a analysis assertion for cross domain transfer.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="DigitalHazMat" type="dhzm:DigitalHazMatType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">A notice on the assertion to inform the
                    user not to decrypt the object, even though they may have the key with the payload,
                    unless they are taking proper precautions.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="ContentCollectionTimestamp"
                type="dhzm:ContentCollectionTimestampType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Date of collection of artifact.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="ContentSize" type="dhzm:ContentSizeType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Size of the entire payload in bytes.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="ContentEncodingMethod" type="dhzm:ContentEncodingMethodType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Encoding to provide obfuscation to original data to prevent accidental execution or
opening.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="ContentEncodedSize" type="dhzm:ContentEncodedSizeType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Size of the encoded content in bytes.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>
```

```
<xs:element name="ContentCollectionHost" type="dhzm:ContentCollectionHostType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">Host collection for artifact.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="ContentCollectionMethod" type="dhzm:ContentCollectionMethodType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">Method of collection for artifact.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="ContentCollectionHostList"
            type="dhzm:ContentCollectionHostListType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">List of hosts collection for artifact.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="ContentCollectionMethodList"
            type="dhzm:ContentCollectionMethodListType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">List of methods of collection for artifact.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="ContentCollectionExternalId"
            type="dhzm:ContentCollectionExternalIdType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">External reference (mission) to collection.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="OriginContentUid" type="dhzm:OriginContentUidType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">User ID of the artifact.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="OriginContentOwner" type="dhzm:OriginContentOwnerType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
```

```
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Owner of the artifact.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>

<xs:element name="OriginContentGroup" type="dhzm:OriginContentGroupType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Group ownership of the artifact.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>

<xs:element name="OriginContentInode" type="dhzm:OriginContentInodeType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Inode of the artifact.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>

<xs:element name="OriginContentDevice" type="dhzm:OriginContentDeviceType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                Any identifier for the device on which the payload artifact was found
                                or from which it was collected. e.g., a filesystem UUID for files collected
                                from a single volume, a hard drive serial number for a disk image, or
                                a MAC for the NIC on which a packet dump was captured.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>

<xs:element name="OriginContentPath" type="dhzm:OriginContentPathType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Full path from the root folder (break for each folder).</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>

<xs:element name="OriginContentPathList" type="dhzm:OriginContentPathListType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">List of full paths from the root folder (break for each folder).</xhtml:p>
                </xs:documentation>
        </xs:annotation>
</xs:element>


<xs:element name="OriginContentFilename" type="dhzm:OriginContentFilenameType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Filename of the artifact.</xhtml:p>
```

```
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentCreated" type="dhzm:OriginContentCreatedType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Date artifact was created (from host filesystem).</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentLastModified"
                type="dhzm:OriginContentLastModifiedType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Date artifact was last modified (from host filesystem).</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentLastAccessed"
                type="dhzm:OriginContentLastAccessedType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Date artifact was last accessed (from host filesystem).</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentOS" type="dhzm:OriginContentOSType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Operating Systems (OS) of where the artifact was collected.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentOSVersion" type="dhzm:OriginContentOSVersionType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">Operating Systems (OS) version of where the artifact was collected.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="OriginContentArch" type="dhzm:OriginContentArchType">
        <xs:annotation>
                <xs:documentation xml:lang="en">
                        <xhtml:p ism:ownerProducer="USA" ism:classification="U">CPU Architecture of where the artifact was collected.</xhtml:p>
                </xs:documentation>
        </xs:annotation>
    </xs:element>
```

```
<xs:element name="OriginContentSourceMac" type="dhzm:OriginContentSourceMacType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">MAC address of where artifact is collected.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="OriginContentSourceIpv4" type="dhzm:OriginContentSourceIpv4Type">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">IPv4 adress of where the artifact is collected.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="OriginContentSourceIpv6" type="dhzm:OriginContentSourceIpv6Type">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">IPv6 adress of where the artifact is collected.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="OriginContentSourceSystem"
            type="dhzm:OriginContentSourceSystemType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">A symbolic name for domain/network (FQDN) where the artifact is collected.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="SourceDomain" type="dhzm:SourceDomainType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">A symbolic name for domain/network where the artifact is sourced.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="DestinationDomain" type="dhzm:DestinationDomainType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">A symbolic name for domain/network where the artifact is destined.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AttackIdList" type="dhzm:AttackIdListType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">List of PRE-ATT&amp;amp;CK, ATT&amp;amp;CK, Mobile IDs.</xhtml:p>
            </xs:documentation>
```

```
        </xs:annotation>
    </xs:element>

    <xs:element name="AttackId" type="dhzm:AttackIdType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">PRE-ATT&amp;amp;CK, ATT&amp;amp;CK, Mobile IDs.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="AnalysisToolDataDate" type="dhzm:AnalysisToolDataDateType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                    The most recent update of data, such as virus signatures, service fingerprints,
                    or similar, used by an analysis tool.
                </xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="AnalysisToolEngine" type="dhzm:AnalysisToolEngineType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                    The engine used to identify the virus scan tool, detonation chamber, static
                    or dynamic analysis tool, or any other analysis tool used to analyze the payload.
                </xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="AnalysisToolVersion" type="dhzm:AnalysisToolVersionType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                    The version number of virus scan tool, detonation chamber, static
                    or dynamic analysis tool, or any other analysis tool used to analyze the payload.
                </xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="KnownMalicious" type="dhzm:KnownMaliciousType">
        <xs:annotation>
            <xs:documentation xml:lang="en">
                <xhtml:p ism:ownerProducer="USA" ism:classification="U">Result of scan of artifact. False or 0 means unknown if malicious.</xhtml:p>
            </xs:documentation>
        </xs:annotation>
    </xs:element>

    <xs:element name="AnalysisToolResultDescription"
                type="dhzm:AnalysisToolResultDescriptionType">
```

```
    <xs:annotation>
        <xs:documentation xml:lang="en">
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">The result of a virus scan, detonation chamber,
                static or dynamic analysis tool, or any other analysis of the payload.
            </xhtml:p>
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalysisMethodList" type="dhzm:AnalysisMethodListType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">List of how was the artifact analyzed.</xhtml:p>
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalysisMethod" type="dhzm:AnalysisMethodType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">How the artifact was analyzed.
                A value of "None" is an explicit statement that no analysis has been performed on the suspect payload.
                A value of "Other" indicates that some form of analysis has been performed,
                but the assertion will not identify what kind, possibly to protect confidential methods.
                Further information may be provided in an dhzm:AnalysisToolResultDescription,
                or the dhzm:WorkFlowID may allow some users to access additional information in other systems.
                A value of "Multiple" indicates that the optional AnalysisMethodToolList would provide
                additional insight as to the methods.
            </xhtml:p>
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalysisTimeFormat" type="dhzm:AnalysisTimeFormatType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">Time format for analysis, timezone mandatory.</xhtml:p>
        </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalysisMethodToolList" type="dhzm:AnalysisMethodToolListType">
    <xs:annotation>
        <xs:documentation xml:lang="en">
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                List of analysis method tools.
                The manual analysis method can be combined with names of tools used by the analyst.
                (e.g., to indicate that the AnalysisToolResultDescription and KnownMalicious values are
                derived from human analysis aided by a reverse engineering tool one might include both
                "ManualAnalysis" and "Ghidra").
            </xhtml:p>
        </xs:documentation>
    </xs:annotation>
</xs:element>
```

```
<xs:element name="AnalysisMethodTool" type="dhzm:AnalysisMethodToolType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:classification="U" ism:ownerProducer="USA">
                            An analysis method tool.
                            The use of registered CPE values is preferred and can be looked up at "https://nvd.nist.gov/products/cpe/search"
                            or offline using the regularly updated dictionaries published at "https://nvd.nist.gov/products/cpe".
                            The use of unregistered CPE values should use "Other:" should be followed by a value in the form of a CPE name,
                            and it should result in submitting a new value for inclusion in the official dictionary,
                            according to the process described at "https://cpe.mitre.org/dictionary/".
                            The use of the manual analysis method (ie. "ManualAnalysis") can be combined with names of tools used by the analyst.
                            (e.g., to indicate that the AnalysisToolResultDescription and KnownMalicious values are
                            derived from human analysis aided by a reverse engineering tool one might include both
                            "ManualAnalysis" and "Ghidra").
                    </xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalysisMethodToolName" type="dhzm:AnalysisMethodToolNameType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">The name of an analysis method tool.</xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

</xs:element>

<xs:element name="WorkFlowId" type="dhzm:WorkFlowIdType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                            An identifier to associate this document with a reference in an external system, such
                            as a project management or ticket tracking tool. Specific meaning is user-defined. When
                            suitable for the use case, an RFC 4122 compliant UUID is recommended.
                    </xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>

<xs:element name="AnalystIdentifier" type="dhzm:AnalystIdentifierType">
    <xs:annotation>
            <xs:documentation xml:lang="en">
                    <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                            The person or team who performed the analysis described by the assertion
                            (e.g., simple names, email addresses for analyst or analysis team,
                            organizational identifiers such as a DOD ID number,
                            UUIDs for pseudonymous attribution, or similar).

                    </xhtml:p>
            </xs:documentation>
    </xs:annotation>
</xs:element>
```

```
        <!--*************************************************-->

<!-- End Elements                                        -->

<!--*************************************************-->


<!--*************************************************-->

<!-- Start Attributes                                    -->

<!--*************************************************-->

<xs:attribute name="DESVersion" type="dhzm:DESVersionType">
           <xs:annotation>
                      <xs:documentation xml:lang="en">
                                 <xhtml:p ism:ownerProducer="USA" ism:classification="U">The version number of the DES.</xhtml:p>
                      </xs:documentation>
           </xs:annotation>
       </xs:attribute>

       <xs:attribute name="analysisMethodToolVersion"
                     type="dhzm:AnalysisMethodToolVersionType">
           <xs:annotation>
                      <xs:documentation xml:lang="en">
                                 <xhtml:p ism:ownerProducer="USA" ism:classification="U">The version of an analysis method tool.</xhtml:p>
                      </xs:documentation>
           </xs:annotation>
       </xs:attribute>

       <!--*************************************************-->

<!--End Attributes                                    -->

<!--*************************************************-->


<!--*************************************************-->

<!--Start Type Definitions                            -->

<!--*************************************************-->

<xs:complexType name="ProvenanceAssertionType">
           <xs:all>
                      <!-- required -->

                      <xs:element ref="dhzm:DigitalHazMat" minOccurs="1" maxOccurs="1"/>
                      <xs:element ref="dhzm:ContentCollectionTimestamp" minOccurs="1" maxOccurs="1"/>
                      <xs:element ref="dhzm:ContentSize" minOccurs="1" maxOccurs="1"/>
                      <xs:element ref="icsfhashv:ContentDecodedHashVerification"
                         minOccurs="1"
                         maxOccurs="1">
                                <xs:annotation>
```

```
                        <xs:documentation xml:lang="en">
                                <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                        Represents the payload in plaintext state.
                                        Hash value is not meant to be taken over the Base64-encoded
                                        state of the payload when used with a Base64Binary payload.
                                </xhtml:p>
                        </xs:documentation>
                </xs:annotation>
        </xs:element>
        <xs:element ref="dhzm:ContentEncodedSize" minOccurs="1" maxOccurs="1"/>
        <xs:element ref="dhzm:ContentEncodingMethod" minOccurs="1" maxOccurs="1"/>
        <xs:element ref="icsfhashv:ContentEncodedHashVerification"
           minOccurs="1"
           maxOccurs="1">
                <xs:annotation>
                        <xs:documentation xml:lang="en">
                                <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                        Represents the hash of the payload in its encrypted state.
                                        Hash value is not meant to be taken over the Base64-encoded
                                        state of the payload when used with a Base64Binary payload.
                                </xhtml:p>
                        </xs:documentation>
                </xs:annotation>
        </xs:element>

        <!-- optional -->

        <xs:element ref="dhzm:ContentCollectionHostList" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:ContentCollectionHostList" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:ContentCollectionMethodList" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:ContentCollectionExternalId" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentUid" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentOwner" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentGroup" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentInode" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentDevice" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentPathList" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentFilename" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentCreated" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentLastModified" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentLastAccessed" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentOS" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentOSVersion" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentArch" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentSourceMac" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentSourceIpv4" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentSourceIpv6" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:OriginContentSourceSystem" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:SourceDomain" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:DestinationDomain" minOccurs="0" maxOccurs="1"/>
                        <xs:element ref="dhzm:WorkFlowId" minOccurs="0" maxOccurs="1"/>
            </xs:all>
            <xs:attribute ref="dhzm:DESVersion" use="required"/>
            <xs:attribute ref="icsf:DESVersion" use="optional"/>
        </xs:complexType>
```

```
<xs:complexType name="AnalysisAssertionType">
    <xs:all>
                <!-- required -->

                <xs:element ref="dhzm:DigitalHazMat" minOccurs="1" maxOccurs="1"/>
                <xs:element ref="dhzm:OriginContentFilename" minOccurs="1" maxOccurs="1"/>
                <xs:element ref="icsfhashv:ContentDecodedHashVerification"
                   minOccurs="1"
                   maxOccurs="1">
                          <xs:annotation>
                                <xs:documentation xml:lang="en">
                                          <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                                    Represents the payload in plaintext state.
                                                    Hash value is not meant to be taken over the Base64-encoded
                                                    state of the payload when used with a Base64Binary payload.
                                          </xhtml:p>
                                </xs:documentation>
                          </xs:annotation>
                </xs:element>
                <xs:element ref="dhzm:KnownMalicious" minOccurs="1" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisMethod" minOccurs="1" maxOccurs="1"/>

                <!-- optional -->

                <xs:element ref="dhzm:AttackIdList" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:OriginContentPathList" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisToolDataDate" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisToolEngine" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisToolVersion" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisToolResultDescription"
                   minOccurs="0"
                   maxOccurs="1"/>
                <xs:element ref="dhzm:AnalysisTimeFormat" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="icsfhashv:ContentEncodedHashVerification"
                   minOccurs="0"
                   maxOccurs="1">
                          <xs:annotation>
                                <xs:documentation xml:lang="en">
                                          <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                                    Represents the hash of the payload in its encrypted state.
                                                    Hash value is not meant to be taken over the Base64-encoded
                                                    state of the payload when used with a Base64Binary payload.
                                          </xhtml:p>
                                </xs:documentation>
                          </xs:annotation>
                </xs:element>
                <xs:element ref="dhzm:AnalysisMethodToolList" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:WorkFlowId" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="dhzm:AnalystIdentifier" minOccurs="0" maxOccurs="1"/>
    </xs:all>
    <xs:attribute ref="dhzm:DESVersion" use="required"/>
    <xs:attribute ref="icsf:DESVersion" use="optional"/>
</xs:complexType>
```

```
<xs:simpleType name="BlockSizeType">
    <xs:restriction base="xs:positiveInteger">
                <xs:minInclusive value="134217728"/>
                <xs:maxInclusive value="536870912"/>
                <xs:enumeration value="134217728"/>
                <xs:enumeration value="268435456"/>
                <xs:enumeration value="536870912"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="HashTypeType">
    <xs:restriction base="xs:string">
                <xs:enumeration value="CRC"/>
                <xs:enumeration value="MD5"/>
                <xs:enumeration value="SHA256"/>
                <xs:enumeration value="SHA384"/>
                <xs:enumeration value="SHA512"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentCollectionTimestampType">
    <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:simpleType name="ContentSizeType">
    <xs:restriction base="xs:integer"/>
</xs:simpleType>

<xs:simpleType name="ContentEncodingMethodType">
    <xs:restriction base="xs:string">
                <xs:enumeration value="XOR"/>
                <xs:enumeration value="ENCRYPTED"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentEncodedSizeType">
    <xs:restriction base="xs:integer"/>
</xs:simpleType>

<xs:simpleType name="DESVersionType">
    <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{6}(\.[0-9]{6})?(\-.{1,23})?"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ContentCollectionHostType">
    <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9_\.-])*"/>
    </xs:restriction>
</xs:simpleType>
```

```
<xs:simpleType name="ContentCollectionMethodType">
    <xs:restriction base="xs:string">
                <xs:enumeration value="LOG"/>
                <xs:enumeration value="FILE"/>
                <xs:enumeration value="MEMORY-DUMP"/>
                <xs:enumeration value="PACKET-CAPTURE"/>
                <xs:enumeration value="OTHER"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ContentCollectionHostListType">
    <xs:sequence>
                <xs:element ref="dhzm:ContentCollectionHost" minOccurs="1" maxOccurs="5"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="ContentCollectionMethodListType">
    <xs:sequence>
                <xs:element ref="dhzm:ContentCollectionMethod" minOccurs="1" maxOccurs="5"/>
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="ContentCollectionExternalIdType">
    <xs:restriction base="xs:anyURI">
                <xs:maxLength value="1024"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentUidType">
    <xs:restriction base="xs:integer">
                <xs:minInclusive value="1"/>
                <xs:maxInclusive value="65335"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentOwnerType">
    <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9\s_-])*"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentGroupType">
    <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9\s_-])*"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentInodeType">
    <xs:restriction base="xs:integer"/>
</xs:simpleType>
```

```
<xs:simpleType name="OriginContentDeviceType">
    <xs:restriction base="xs:string">
            <xs:maxLength value="255"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentPathType">
    <xs:restriction base="xs:anyURI">
            <xs:maxLength value="1024"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="OriginContentPathListType">
    <xs:sequence>
            <xs:element ref="dhzm:OriginContentPath" minOccurs="1" maxOccurs="256"/>
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="OriginContentFilenameType">
    <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1024"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentCreatedType">
    <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:simpleType name="OriginContentLastModifiedType">
    <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:simpleType name="OriginContentLastAccessedType">
    <xs:restriction base="xs:dateTime"/>
</xs:simpleType>

<xs:simpleType name="OriginContentOSType">
    <!-- NOTE: need to add to list, these are just examples -->

    <xs:restriction base="xs:string">
            <xs:enumeration value="windows"/>
            <xs:enumeration value="macOS"/>
            <xs:enumeration value="linux"/>
            <xs:enumeration value="android"/>
            <xs:enumeration value="iOS"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="OriginContentOSVersionType">
    <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="255"/>
```

```
                <xs:pattern value="([a-zA-Z0-9\.-])*"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="OriginContentArchType">
            <xs:restriction base="xs:string">
                <xs:enumeration value="i386"/>
                <xs:enumeration value="i486"/>
                <xs:enumeration value="i586"/>
                <xs:enumeration value="i686"/>
                <xs:enumeration value="x86_64"/>
                <xs:enumeration value="amd64"/>
                <xs:enumeration value="ia64"/>
                <xs:enumeration value="armv6l"/>
                <xs:enumeration value="armv7l"/>
                <xs:enumeration value="sparc"/>
                <xs:enumeration value="sparc64"/>
                <xs:enumeration value="sparc64v"/>
                <xs:enumeration value="ppc"/>
                <xs:enumeration value="ppc64"/>
                <xs:enumeration value="ppc64le"/>
                <xs:enumeration value="s390"/>
                <xs:enumeration value="s390x"/>
                <xs:enumeration value="64-bit"/>
                <xs:enumeration value="32-bit"/>
                <xs:enumeration value="none"/>
                <xs:enumeration value="noarch"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="OriginContentSourceMacType">
            <xs:restriction base="xs:hexBinary">
                <xs:minLength value="6"/>
                <xs:maxLength value="7"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="OriginContentSourceIpv4Type">
            <xs:annotation>
                <xs:documentation>
                    <xhtml:p>A four-byte IPv4 address of the system where the payload was collected.</xhtml:p>
                </xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:hexBinary">
                <xs:length value="4"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="OriginContentSourceIpv6Type">
            <xs:annotation>
                <xs:documentation>
                    <xhtml:p>A 16-byte IPv6 address of the system where the payload was collected.</xhtml:p>
                </xs:documentation>
            </xs:annotation>
```

```
        <xs:restriction base="xs:hexBinary">
                <xs:length value="16"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="OriginContentSourceSystemType">
        <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9\._-])*"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="SourceDomainType">
        <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9])*"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="DestinationDomainType">
        <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9])*"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="AttackIdListType">
        <xs:sequence>
                <xs:element ref="dhzm:AttackId" minOccurs="1" maxOccurs="4096"/>
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="AttackIdType">
        <xs:restriction base="xs:string">
                <xs:pattern value="TA?[0-9]{4}"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="AnalysisToolDataDateType">
        <xs:restriction base="xs:dateTime"/>
    </xs:simpleType>

    <xs:simpleType name="AnalysisToolEngineType">
        <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="255"/>
                <xs:pattern value="([a-zA-Z0-9])*"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="AnalysisToolVersionType">
```

```
            <xs:restriction base="xs:string">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="255"/>
                        <xs:pattern value="([a-zA-Z0-9\.-])*"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="KnownMaliciousType">
            <xs:restriction base="xs:boolean"/>
        </xs:simpleType>

        <xs:simpleType name="AnalysisToolResultDescriptionType">
            <xs:restriction base="xs:string">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="255"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:complexType name="AnalysisMethodListType">
            <xs:sequence>
                        <xs:element ref="dhzm:AnalysisMethod" minOccurs="1" maxOccurs="256"/>
            </xs:sequence>
        </xs:complexType>

        <xs:simpleType name="AnalysisMethodType">
            <xs:union memberTypes="AnalysisMethodEnumerationType">
                        <xs:simpleType>
                                    <xs:restriction base="xs:string">
                                          <xs:minLength value="1"/>
                                          <xs:maxLength value="255"/>
                                          <xs:pattern value="([a-zA-Z0-9])*"/>
                                    </xs:restriction>
                        </xs:simpleType>
            </xs:union>
        </xs:simpleType>

        <xs:simpleType name="AnalysisMethodEnumerationType">
            <xs:restriction base="xs:string">
                        <xs:enumeration value="Virus_Scan"/>
                        <xs:enumeration value="Detonation_Chamber"/>
                        <xs:enumeration value="Reverse_Engineering"/>
                        <xs:enumeration value="Manual_Review"/>
                        <xs:enumeration value="Multiple"/>
                        <xs:enumeration value="Other"/>
                        <xs:enumeration value="None"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="AnalysisTimeFormatType">
            <xs:restriction base="xs:dateTime">
                        <xs:pattern value=".{20}.*"/>
            </xs:restriction>
        </xs:simpleType>
```

```
<xs:complexType name="AnalysisMethodToolListType">
    <xs:sequence>
                <xs:element ref="dhzm:AnalysisMethodTool" minOccurs="1" maxOccurs="256"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="AnalysisMethodToolType">
    <xs:sequence>
                <xs:element ref="dhzm:AnalysisMethodToolName" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute ref="dhzm:analysisMethodToolVersion"/>
</xs:complexType>

<xs:simpleType name="AnalysisMethodToolNameType">
    <xs:union memberTypes="dhzm:AnalysisMethodToolNameEnumeratedType dhzm:RegisteredCPEType dhzm:UnregisteredCPEType"/>
</xs:simpleType>

<xs:simpleType name="AnalysisMethodToolNameEnumeratedType">
    <xs:restriction base="xs:string">
                <xs:enumeration value="ManualAnalysis"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RegisteredCPEType">
    <xs:annotation>
                <xs:documentation xml:lang="en">
                            <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                        The regular expressions OR'ed together in this
                                        type were copied verbatim from the cpe22Type and
                                        cpe23Type definitions in
                                        <xhtml:a xhtml:href="https://csrc.nist.gov/schema/cpe/2.3/cpe-naming_2.3.xsd">
                                                    the official CPE schema
                                        </xhtml:a>
                                        . The length restriction is added to constrain
                                        the values to a reasonable length for cross-domain
                                        use.
                            </xhtml:p>
                </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:anyURI">
                <xs:minLength value="1"/>
                <xs:maxLength value="1024"/>
                <xs:pattern value="([c][pP][eE]:/[AHOaho]?(:[A-Za-z0-9\._\-~%]*){0,6})|(cpe:2\.3:[aho\*\-](:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&#34;#$$%&amp;'\(\)\
+,/:;&lt;=&gt;@\[\]\^\`\{\|}~]))+(\?*|\*?))|[\*\-])){5}(:(([a-zA-Z]{2,3}(-([a-zA-Z]{2}|[0-9]{3}))?)|[\*\-]))(:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&#34;#$$%&amp;'\(\)\+,/:;&lt;=&gt;@\[\]\^\`\
{\|}~]))+(\?*|\*?))|[\*\-])){4})"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="UnregisteredCPEType">
    <xs:annotation>
                <xs:documentation xml:lang="en">
                            <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                                        Unregistered CPE has "Other:" as a prefix on the cpe22Type and cpe23Type regex.
                                        The regular expressions OR'ed together in this
```

```
                                        type were copied verbatim from the cpe22Type and
                                        cpe23Type definitions in
                                        <xhtml:a xhtml:href="https://csrc.nist.gov/schema/cpe/2.3/cpe-naming_2.3.xsd">
                                                the official CPE schema
                                        </xhtml:a>
                                        . The length restriction is added to constrain
                                        the values to a reasonable length for cross-domain
                                        use.
                                </xhtml:p>
                        </xs:documentation>
                </xs:annotation>
                <xs:restriction base="xs:anyURI">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="1024"/>
                        <xs:pattern value="Other:([c][pP][eE]:/[AHOaho]?(:[A-Za-z0-9\._\-~%]*){0,6})|Other:(cpe:2\.3:[aho\*\-](:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&#34;#$$%&amp;'\
(\)\+,/:;&lt;=&gt;@\[\]\^\`\{\|}~]))+(\?*|\*?))|[\*\-])){5}(:(([a-zA-Z]{2,3}(-([a-zA-Z]{2}|[0-9]{3}))?)|[\*\-]))(:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&#34;#$$%&amp;'\(\)\+,/:;&lt;=&gt;@\[\]
\^\`\{\|}~]))+(\?*|\*?))|[\*\-])){4})"/>
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="AnalysisMethodToolVersionType">
                <xs:restriction base="xs:string">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="255"/>
                        <xs:pattern value="([a-zA-Z0-9\.-])*"/>
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="DigitalHazMatType">
                <xs:restriction base="xs:string">
                        <xs:pattern value="\s*This\s+element\s+describes\s+an\s+obfuscated\s+payload\s+which\s+is\s+either\s+known\s+or\s+suspected\s+to\s+contain\s+software\s+or\s
+similar\s+data\s+which\s+could\s+cause\s+harm\s+to\s+information\s+processing\s+systems\.\s+It\s+has\s+been\s+encapsulated\s+to\s+render\s+it\s+inert\.\s+Any\s+attempt\s+to\s+decode\s+this\s
+payload\s+outside\s+a\s+safe\s+analysis\s+environment\s+may\s+pose\s+a\s+danger\s+to\s+your\s+system\.\s*"/>
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="WorkFlowIdType">
                <xs:restriction base="xs:string">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="255"/>
                        <xs:pattern value="([a-zA-Z0-9\s:\._-])*"/>
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="AnalystIdentifierType">
                <xs:restriction base="xs:string">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="1024"/>
                </xs:restriction>
        </xs:simpleType>

        <!--**************************************************-->

<!--End Type Definitions                                 -->
```

```
<!--**************************************************-->

<xs:annotation>
          <xs:documentation>
                    <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Formal Change List</xhtml:h2>
                    <xhtml:table ism:ownerProducer="USA" ism:classification="U" id="ChangeHistory">
                              <xhtml:caption>Change History</xhtml:caption>
                              <xhtml:thead>
                                        <xhtml:tr>
                                                  <xhtml:th>Version</xhtml:th>
                                                  <xhtml:th>Date</xhtml:th>
                                                  <xhtml:th>By</xhtml:th>
                                                  <xhtml:th>Description</xhtml:th>
                                        </xhtml:tr>
                              </xhtml:thead>
                              <xhtml:tbody>
                                        <xhtml:tr>
                                                  <xhtml:td>2021-JAN</xhtml:td>
                                                  <xhtml:td>2020-12-01</xhtml:td>
                                                  <xhtml:td>ODNI/CIO/IAD</xhtml:td>
                                                  <xhtml:td>Initial creation, reference the change history in the DES.</xhtml:td>
                                        </xhtml:tr>
                              </xhtml:tbody>
                    </xhtml:table>
          </xs:documentation>
       </xs:annotation>
    </xs:schema>
```

2.2 - DHZM-guard.xsd

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns="urn:us:gov:ic:digitalhazmat"
                        xmlns:dhzm="urn:us:gov:ic:digitalhazmat"
                        xmlns:tdf="urn:us:gov:ic:tdf"
                        xmlns:icsfhashv="urn:us:gov:ic:sf:hashverification"
                        xmlns:icsf="urn:us:gov:ic:sf"
                        targetNamespace="urn:us:gov:ic:digitalhazmat"
                        elementFormDefault="qualified"
                        attributeFormDefault="qualified"
                        version="202101">
                <xs:import namespace="urn:us:gov:ic:sf:hashverification"
                           schemaLocation="../IC-SF/HashVerification.xsd"/>
                <xs:import namespace="urn:us:gov:ic:sf" schemaLocation="../IC-SF/IC-SF.xsd"/>
                <xs:element name="ProvenanceAssertion" type="dhzm:ProvenanceAssertionType"/>
                <xs:element name="AnalysisAssertion" type="dhzm:AnalysisAssertionType"/>
                <xs:element name="DigitalHazMat" type="dhzm:DigitalHazMatType"/>
                <xs:element name="ContentCollectionTimestamp"
                            type="dhzm:ContentCollectionTimestampType"/>
                <xs:element name="ContentSize" type="dhzm:ContentSizeType"/>
                <xs:element name="ContentEncodingMethod" type="dhzm:ContentEncodingMethodType"/>
                <xs:element name="ContentEncodedSize" type="dhzm:ContentEncodedSizeType"/>
                <xs:element name="ContentCollectionHost" type="dhzm:ContentCollectionHostType"/>
                <xs:element name="ContentCollectionMethod" type="dhzm:ContentCollectionMethodType"/>
                <xs:element name="ContentCollectionHostList"
                            type="dhzm:ContentCollectionHostListType"/>
                <xs:element name="ContentCollectionMethodList"
                            type="dhzm:ContentCollectionMethodListType"/>
                <xs:element name="ContentCollectionExternalId"
                            type="dhzm:ContentCollectionExternalIdType"/>
                <xs:element name="OriginContentUid" type="dhzm:OriginContentUidType"/>
                <xs:element name="OriginContentOwner" type="dhzm:OriginContentOwnerType"/>
                <xs:element name="OriginContentGroup" type="dhzm:OriginContentGroupType"/>
                <xs:element name="OriginContentInode" type="dhzm:OriginContentInodeType"/>
                <xs:element name="OriginContentDevice" type="dhzm:OriginContentDeviceType"/>
                <xs:element name="OriginContentPath" type="dhzm:OriginContentPathType"/>
                <xs:element name="OriginContentPathList" type="dhzm:OriginContentPathListType"/>
                <xs:element name="OriginContentFilename" type="dhzm:OriginContentFilenameType"/>
                <xs:element name="OriginContentCreated" type="dhzm:OriginContentCreatedType"/>
                <xs:element name="OriginContentLastModified"
                            type="dhzm:OriginContentLastModifiedType"/>
                <xs:element name="OriginContentLastAccessed"
                            type="dhzm:OriginContentLastAccessedType"/>
                <xs:element name="OriginContentOS" type="dhzm:OriginContentOSType"/>
                <xs:element name="OriginContentOSVersion" type="dhzm:OriginContentOSVersionType"/>
                <xs:element name="OriginContentArch" type="dhzm:OriginContentArchType"/>
                <xs:element name="OriginContentSourceMac" type="dhzm:OriginContentSourceMacType"/>
                <xs:element name="OriginContentSourceIpv4" type="dhzm:OriginContentSourceIpv4Type"/>
                <xs:element name="OriginContentSourceIpv6" type="dhzm:OriginContentSourceIpv6Type"/>
                <xs:element name="OriginContentSourceSystem"
                            type="dhzm:OriginContentSourceSystemType"/>
                <xs:element name="SourceDomain" type="dhzm:SourceDomainType"/>
                <xs:element name="DestinationDomain" type="dhzm:DestinationDomainType"/>
```

```
<xs:element name="AttackIdList" type="dhzm:AttackIdListType"/>
<xs:element name="AttackId" type="dhzm:AttackIdType"/>
<xs:element name="AnalysisToolDataDate" type="dhzm:AnalysisToolDataDateType"/>
<xs:element name="AnalysisToolEngine" type="dhzm:AnalysisToolEngineType"/>
<xs:element name="AnalysisToolVersion" type="dhzm:AnalysisToolVersionType"/>
<xs:element name="KnownMalicious" type="dhzm:KnownMaliciousType"/>
<xs:element name="AnalysisToolResultDescription"
            type="dhzm:AnalysisToolResultDescriptionType"/>
<xs:element name="AnalysisMethodList" type="dhzm:AnalysisMethodListType"/>
<xs:element name="AnalysisMethod" type="dhzm:AnalysisMethodType"/>
<xs:element name="AnalysisTimeFormat" type="dhzm:AnalysisTimeFormatType"/>
<xs:element name="AnalysisMethodToolList" type="dhzm:AnalysisMethodToolListType"/>
<xs:element name="AnalysisMethodTool" type="dhzm:AnalysisMethodToolType"/>
<xs:element name="AnalysisMethodToolName" type="dhzm:AnalysisMethodToolNameType"/>
<xs:element name="WorkFlowId" type="dhzm:WorkFlowIdType"/>
<xs:element name="AnalystIdentifier" type="dhzm:AnalystIdentifierType"/>
<xs:attribute name="DESVersion" type="dhzm:DESVersionType"/>
<xs:attribute name="analysisMethodToolVersion"
              type="dhzm:AnalysisMethodToolVersionType"/>
<xs:complexType name="ProvenanceAssertionType">
   <xs:all>
      <xs:element ref="dhzm:DigitalHazMat"/>
      <xs:element ref="dhzm:ContentCollectionTimestamp"/>
      <xs:element ref="dhzm:ContentSize"/>
      <xs:element ref="icsfhashv:ContentDecodedHashVerification"/>
      <xs:element ref="dhzm:ContentEncodedSize"/>
      <xs:element ref="dhzm:ContentEncodingMethod"/>
      <xs:element ref="icsfhashv:ContentEncodedHashVerification"/>
      <xs:element ref="dhzm:ContentCollectionHostList" minOccurs="0"/>
      <xs:element ref="dhzm:ContentCollectionMethodList" minOccurs="0"/>
      <xs:element ref="dhzm:ContentCollectionExternalId" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentUid" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentOwner" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentGroup" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentInode" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentDevice" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentPathList" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentFilename" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentCreated" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentLastModified" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentLastAccessed" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentOS" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentOSVersion" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentArch" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentSourceMac" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentSourceIpv4" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentSourceIpv6" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentSourceSystem" minOccurs="0"/>
      <xs:element ref="dhzm:SourceDomain" minOccurs="0"/>
      <xs:element ref="dhzm:DestinationDomain" minOccurs="0"/>
      <xs:element ref="dhzm:WorkFlowId" minOccurs="0"/>
   </xs:all>
   <xs:attribute ref="dhzm:DESVersion" use="required"/>
   <xs:attribute ref="icsf:DESVersion" use="optional"/>
```

```
</xs:complexType>
<xs:complexType name="AnalysisAssertionType">
   <xs:all>
      <xs:element ref="dhzm:DigitalHazMat"/>
      <xs:element ref="dhzm:OriginContentFilename"/>
      <xs:element ref="icsfhashv:ContentDecodedHashVerification"/>
      <xs:element ref="dhzm:KnownMalicious"/>
      <xs:element ref="dhzm:AnalysisMethod"/>
      <xs:element ref="dhzm:AttackIdList" minOccurs="0"/>
      <xs:element ref="dhzm:OriginContentPathList" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisToolDataDate" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisToolEngine" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisToolVersion" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisToolResultDescription" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisTimeFormat" minOccurs="0"/>
      <xs:element ref="icsfhashv:ContentEncodedHashVerification" minOccurs="0"/>
      <xs:element ref="dhzm:AnalysisMethodToolList" minOccurs="0"/>
      <xs:element ref="dhzm:WorkFlowId" minOccurs="0"/>
      <xs:element ref="dhzm:AnalystIdentifier" minOccurs="0"/>
   </xs:all>
   <xs:attribute ref="dhzm:DESVersion" use="required"/>
   <xs:attribute ref="icsf:DESVersion" use="optional"/>
</xs:complexType>
<xs:simpleType name="BlockSizeType">
   <xs:restriction base="xs:positiveInteger">
      <xs:minInclusive value="134217728"/>
      <xs:maxInclusive value="536870912"/>
      <xs:enumeration value="134217728"/>
      <xs:enumeration value="268435456"/>
      <xs:enumeration value="536870912"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="HashTypeType">
   <xs:restriction base="xs:string">
      <xs:enumeration value="CRC"/>
      <xs:enumeration value="MD5"/>
      <xs:enumeration value="SHA256"/>
      <xs:enumeration value="SHA384"/>
      <xs:enumeration value="SHA512"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="ContentCollectionTimestampType">
   <xs:restriction base="xs:dateTime"/>
</xs:simpleType>
<xs:simpleType name="ContentSizeType">
   <xs:restriction base="xs:integer"/>
</xs:simpleType>
<xs:simpleType name="ContentEncodingMethodType">
   <xs:restriction base="xs:string">
      <xs:enumeration value="XOR"/>
      <xs:enumeration value="ENCRYPTED"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="ContentEncodedSizeType">
```

```
      <xs:restriction base="xs:integer"/>
   </xs:simpleType>
   <xs:simpleType name="DESVersionType">
      <xs:restriction base="xs:string">
         <xs:pattern value="[0-9]{6}(\.[0-9]{6})?(\-.{1,23})?"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="ContentCollectionHostType">
      <xs:restriction base="xs:string">
         <xs:minLength value="1"/>
         <xs:maxLength value="255"/>
         <xs:pattern value="([a-zA-Z0-9_\.-])*"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="ContentCollectionMethodType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="LOG"/>
         <xs:enumeration value="FILE"/>
         <xs:enumeration value="MEMORY-DUMP"/>
         <xs:enumeration value="PACKET-CAPTURE"/>
         <xs:enumeration value="OTHER"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:complexType name="ContentCollectionHostListType">
      <xs:sequence>
         <xs:element ref="dhzm:ContentCollectionHost" maxOccurs="5"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="ContentCollectionMethodListType">
      <xs:sequence>
         <xs:element ref="dhzm:ContentCollectionMethod" maxOccurs="5"/>
      </xs:sequence>
   </xs:complexType>
   <xs:simpleType name="ContentCollectionExternalIdType">
      <xs:restriction base="xs:anyURI">
         <xs:maxLength value="1024"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentUidType">
      <xs:restriction base="xs:integer">
         <xs:minInclusive value="1"/>
         <xs:maxInclusive value="65335"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentOwnerType">
      <xs:restriction base="xs:string">
         <xs:minLength value="1"/>
         <xs:maxLength value="255"/>
         <xs:pattern value="([a-zA-Z0-9\s_-])*"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentGroupType">
      <xs:restriction base="xs:string">
         <xs:minLength value="1"/>
```

```
            <xs:maxLength value="255"/>
            <xs:pattern value="([a-zA-Z0-9\s_-])*"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:simpleType name="OriginContentInodeType">
         <xs:restriction base="xs:integer"/>
      </xs:simpleType>
      <xs:simpleType name="OriginContentDeviceType">
         <xs:restriction base="xs:string">
            <xs:maxLength value="255"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:simpleType name="OriginContentPathType">
         <xs:restriction base="xs:anyURI">
            <xs:maxLength value="1024"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:complexType name="OriginContentPathListType">
         <xs:sequence>
            <xs:element ref="dhzm:OriginContentPath" maxOccurs="256"/>
         </xs:sequence>
      </xs:complexType>
      <xs:simpleType name="OriginContentFilenameType">
         <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="1024"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:simpleType name="OriginContentCreatedType">
         <xs:restriction base="xs:dateTime"/>
      </xs:simpleType>
      <xs:simpleType name="OriginContentLastModifiedType">
         <xs:restriction base="xs:dateTime"/>
      </xs:simpleType>
      <xs:simpleType name="OriginContentLastAccessedType">
         <xs:restriction base="xs:dateTime"/>
      </xs:simpleType>
      <xs:simpleType name="OriginContentOSType">
         <xs:restriction base="xs:string">
            <xs:enumeration value="windows"/>
            <xs:enumeration value="macOS"/>
            <xs:enumeration value="linux"/>
            <xs:enumeration value="android"/>
            <xs:enumeration value="iOS"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:simpleType name="OriginContentOSVersionType">
         <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="255"/>
            <xs:pattern value="([a-zA-Z0-9\.-])*"/>
         </xs:restriction>
      </xs:simpleType>
      <xs:simpleType name="OriginContentArchType">
```

```
      <xs:restriction base="xs:string">
         <xs:enumeration value="i386"/>
         <xs:enumeration value="i486"/>
         <xs:enumeration value="i586"/>
         <xs:enumeration value="i686"/>
         <xs:enumeration value="x86_64"/>
         <xs:enumeration value="amd64"/>
         <xs:enumeration value="ia64"/>
         <xs:enumeration value="armv6l"/>
         <xs:enumeration value="armv7l"/>
         <xs:enumeration value="sparc"/>
         <xs:enumeration value="sparc64"/>
         <xs:enumeration value="sparc64v"/>
         <xs:enumeration value="ppc"/>
         <xs:enumeration value="ppc64"/>
         <xs:enumeration value="ppc64le"/>
         <xs:enumeration value="s390"/>
         <xs:enumeration value="s390x"/>
         <xs:enumeration value="64-bit"/>
         <xs:enumeration value="32-bit"/>
         <xs:enumeration value="none"/>
         <xs:enumeration value="noarch"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentSourceMacType">
      <xs:restriction base="xs:hexBinary">
         <xs:minLength value="6"/>
         <xs:maxLength value="7"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentSourceIpv4Type">
      <xs:restriction base="xs:hexBinary">
         <xs:length value="4"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentSourceIpv6Type">
      <xs:restriction base="xs:hexBinary">
         <xs:length value="16"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="OriginContentSourceSystemType">
      <xs:restriction base="xs:string">
         <xs:minLength value="1"/>
         <xs:maxLength value="255"/>
         <xs:pattern value="([a-zA-Z0-9\._-])*"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="SourceDomainType">
      <xs:restriction base="xs:string">
         <xs:minLength value="1"/>
         <xs:maxLength value="255"/>
         <xs:pattern value="([a-zA-Z0-9])*"/>
      </xs:restriction>
   </xs:simpleType>
```

```
<xs:simpleType name="DestinationDomainType">
   <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="255"/>
      <xs:pattern value="([a-zA-Z0-9])*"/>
   </xs:restriction>
</xs:simpleType>
<xs:complexType name="AttackIdListType">
   <xs:sequence>
      <xs:element ref="dhzm:AttackId" maxOccurs="4096"/>
   </xs:sequence>
</xs:complexType>
<xs:simpleType name="AttackIdType">
   <xs:restriction base="xs:string">
      <xs:pattern value="TA?[0-9]{4}"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="AnalysisToolDataDateType">
   <xs:restriction base="xs:dateTime"/>
</xs:simpleType>
<xs:simpleType name="AnalysisToolEngineType">
   <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="255"/>
      <xs:pattern value="([a-zA-Z0-9])*"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="AnalysisToolVersionType">
   <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="255"/>
      <xs:pattern value="([a-zA-Z0-9\.-])*"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="KnownMaliciousType">
   <xs:restriction base="xs:boolean"/>
</xs:simpleType>
<xs:simpleType name="AnalysisToolResultDescriptionType">
   <xs:restriction base="xs:string">
      <xs:minLength value="1"/>
      <xs:maxLength value="255"/>
   </xs:restriction>
</xs:simpleType>
<xs:complexType name="AnalysisMethodListType">
   <xs:sequence>
      <xs:element ref="dhzm:AnalysisMethod" maxOccurs="256"/>
   </xs:sequence>
</xs:complexType>
<xs:simpleType name="AnalysisMethodType">
   <xs:union memberTypes="AnalysisMethodEnumerationType">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="255"/>
```

```
            <xs:pattern value="([a-zA-Z0-9])*"/>
         </xs:restriction>
      </xs:simpleType>
   </xs:union>
</xs:simpleType>
<xs:simpleType name="AnalysisMethodEnumerationType">
   <xs:restriction base="xs:string">
      <xs:enumeration value="Virus_Scan"/>
      <xs:enumeration value="Detonation_Chamber"/>
      <xs:enumeration value="Reverse_Engineering"/>
      <xs:enumeration value="Manual_Review"/>
      <xs:enumeration value="Multiple"/>
      <xs:enumeration value="Other"/>
      <xs:enumeration value="None"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="AnalysisTimeFormatType">
   <xs:restriction base="xs:dateTime">
      <xs:pattern value=".{20}.*"/>
   </xs:restriction>
</xs:simpleType>
<xs:complexType name="AnalysisMethodToolListType">
   <xs:sequence>
      <xs:element ref="dhzm:AnalysisMethodTool" maxOccurs="256"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="AnalysisMethodToolType">
   <xs:sequence>
      <xs:element ref="dhzm:AnalysisMethodToolName"/>
   </xs:sequence>
   <xs:attribute ref="dhzm:analysisMethodToolVersion"/>
</xs:complexType>
<xs:simpleType name="AnalysisMethodToolNameType">
   <xs:union memberTypes="dhzm:AnalysisMethodToolNameEnumeratedType dhzm:RegisteredCPEType dhzm:UnregisteredCPEType"/>
</xs:simpleType>
<xs:simpleType name="AnalysisMethodToolNameEnumeratedType">
   <xs:restriction base="xs:string">
      <xs:enumeration value="ManualAnalysis"/>
   </xs:restriction>
</xs:simpleType>
<xs:simpleType name="RegisteredCPEType">
   <xs:restriction base="xs:anyURI">
      <xs:minLength value="1"/>
      <xs:maxLength value="1024"/>
      <xs:pattern value="([c][pP][eE]:/[AHOaho]?(:[A-Za-z0-9\._\-~%]*){0,6})|(cpe:2\.3:[aho\*\-](:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&amp;#34;#$$%&amp;amp;'\(\)\+,/:;&amp;lt;=&amp;gt;@\
[\]\^`\{\|}~]))+(\?*|\*?))|[\*\-])){5}(:(([a-zA-Z]{2,3}(-([a-zA-Z]{2}|[0-9]{3}))?)|[\*\-]))(:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&amp;#34;#$$%&amp;amp;'\(\)\+,/:;&amp;lt;=&amp;gt;@\[\]\^`\{\|}~]))+(\?*|
\*?))|[\*\-])){4})"/>
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="UnregisteredCPEType">
      <xs:restriction base="xs:anyURI">
         <xs:minLength value="1"/>
         <xs:maxLength value="1024"/>
         <xs:pattern value="Other:([c][pP][eE]:/[AHOaho]?(:[A-Za-z0-9\._\-~%]*){0,6})|Other:(cpe:2\.3:[aho\*\-](:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&amp;#34;#$$%&amp;amp;'\(\)\
```

```
+,/:;&lt;=&gt;@\[\]\^`\{\|}~]))+(\?*|\*?))|[\*\-])){5}(:(([a-zA-Z]{2,3}(-([a-zA-Z]{2}|[0-9]{3}))?)|[\*\-]))(:(((\?*|\*?)([a-zA-Z0-9\-\._]|(\\[\\\*\?!&#34;#$$%&amp;'\(\)\+,/:;&lt;=&gt;@\[\]\^`\
{\|}~]))+(\?*|\*?))|[\*\-])){4})"/>
                  </xs:restriction>
               </xs:simpleType>
               <xs:simpleType name="AnalysisMethodToolVersionType">
                  <xs:restriction base="xs:string">
                     <xs:minLength value="1"/>
                     <xs:maxLength value="255"/>
                     <xs:pattern value="([a-zA-Z0-9\.-])*"/>
                  </xs:restriction>
               </xs:simpleType>
               <xs:simpleType name="DigitalHazMatType">
                  <xs:restriction base="xs:string">
                     <xs:pattern value="\s*This\s+element\s+describes\s+an\s+obfuscated\s+payload\s+which\s+is\s+either\s+known\s+or\s+suspected\s+to\s+contain\s+software\s+or\s+similar\s
+data\s+which\s+could\s+cause\s+harm\s+to\s+information\s+processing\s+systems\.\s+It\s+has\s+been\s+encapsulated\s+to\s+render\s+it\s+inert\.\s+Any\s+attempt\s+to\s+decode\s+this\s+payload\s
+outside\s+a\s+safe\s+analysis\s+environment\s+may\s+pose\s+a\s+danger\s+to\s+your\s+system\.\s*"/>
                  </xs:restriction>
               </xs:simpleType>
               <xs:simpleType name="WorkFlowIdType">
                  <xs:restriction base="xs:string">
                     <xs:minLength value="1"/>
                     <xs:maxLength value="255"/>
                     <xs:pattern value="([a-zA-Z0-9\s:\._-])*"/>
                  </xs:restriction>
               </xs:simpleType>
               <xs:simpleType name="AnalystIdentifierType">
                  <xs:restriction base="xs:string">
                     <xs:minLength value="1"/>
                     <xs:maxLength value="1024"/>
                  </xs:restriction>
               </xs:simpleType>
            </xs:schema>
```

2.3 - SchemaGuideSchema.xsd

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                           xmlns:xhtml="http://www.w3.org/1999/xhtml-StopBrowserRendering"
                           attributeFormDefault="qualified"
                           ism:compliesWith="USGov USIC"
                           ism:resourceElement="true"
                           ism:createDate="2019-09-18"
                           ism:DESVersion="201903.202010"
                           ism:ISMCATCESVersion="202010"
                           ism:classification="U"
                           ism:ownerProducer="USA"
                           version="202101"
                           elementFormDefault="qualified"
                           targetNamespace="urn:schema:guide:schema:digitalhazmat"
                           xml:lang="en">
                 <xsd:annotation>
                    <xsd:documentation>
                       <xhtml:h1 ism:ownerProducer="USA" ism:classification="U">Intelligence Community
              Technical Specification XML Data Encoding Specification for DigitalHazMat Assertion (DHZM.XML) SchemaGuide</xhtml:h1>
                    </xsd:documentation>

                    <xsd:documentation>
                       <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Notices</xhtml:h2>
                       <xhtml:p ism:ownerProducer="USA" ism:classification="U"> Distribution Notice:
           This document has been approved for Public Release and is available for use without restriction.

            </xhtml:p>
            </xsd:documentation>
            <xsd:documentation>
               <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Description</xhtml:h2>
               <xhtml:p ism:ownerProducer="USA" ism:classification="U"> W3C XML Schema used to
        facilitate generation of the SchemaGuide for the XML Data Encoding Specification for
        DigitalHazMat Assertion (DHZM.XML). </xhtml:p>
            </xsd:documentation>
            <xsd:documentation>
               <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Introduction</xhtml:h2>
               <xhtml:p ism:ownerProducer="USA" ism:classification="U"> This XML Schema file is only
        used to produce the schemaGuide for the XML Data Encoding Specification (DES).
        Please see the document titled <xhtml:i>
                     <xhtml:a href="../../Documents/DHZM/DesDhzmXml.pdf">XML Data Encoding Specification for
               DigitalHazMat Assertion
               (DHZM.XML)</xhtml:a>
                  </xhtml:i> for a complete description of the encoding as well as list of all
        components. </xhtml:p>
               <xhtml:p ism:ownerProducer="USA" ism:classification="U"> It is envisioned that this
        schema or its components, as well as other parts of the DES may be overridden for
        localized implementations. Therefore, permission to use, copy, modify and distribute
        this XML Schema and the other parts of the DES for any purpose is hereby granted in
        perpetuity. </xhtml:p>
               <xhtml:p ism:ownerProducer="USA" ism:classification="U"> Please reference the preceding
        two paragraphs in all copies or variations. The developers make no representation
        about the suitability of the schema or DES for any purpose. It is provided "as is"
        without expressed or implied warranty. </xhtml:p>
```

```
            <xhtml:p ism:ownerProducer="USA" ism:classification="U"> If you modify this XML Schema
in any way label your schema as a variant of
(DHZM.XML). </xhtml:p>
            <xhtml:p ism:ownerProducer="USA" ism:classification="U"> Please direct all questions,
bug reports,or suggestions for changes to the points of contact identified in the
document referenced above. </xhtml:p>
         </xsd:documentation>
         <xsd:documentation>
            <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Implementation Notes</xhtml:h2>
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">A DHZM.XML instance is an
instance of a DHZMC-TDO or a TDO with particular payload and assertions. Its structure is similar
to:</xhtml:p>
            <xhtml:ul>
               <xhtml:p ism:ownerProducer="USA" ism:classification="U">
                  <xhtml:a href="DHZMC-TDF_xsd_Element_TrustedDataObject.html#TrustedDataObject">
            tdf:TrustedDataObject</xhtml:a> and has the following assertions:
</xhtml:p>
               <xhtml:ul>
                  <xhtml:li ism:ownerProducer="USA" ism:classification="U">
                     <xhtml:a href="DHZM_xsd_Element_ProvenanceAssertion.html#ProvenanceAssertion">dhzm:ProvenanceAssertion</xhtml:a>
                  </xhtml:li>
                  <xhtml:li ism:ownerProducer="USA" ism:classification="U">
                     <xhtml:a href="DHZM_xsd_Element_AnalysisAssertion.html#AnalysisAssertion">dhzm:AnalysisAssertion</xhtml:a>
                  </xhtml:li>
               </xhtml:ul>
            </xhtml:ul>
         </xsd:documentation>
         <xsd:documentation>
            <xhtml:h2 ism:ownerProducer="USA" ism:classification="U">Creators</xhtml:h2>
            <xhtml:p ism:ownerProducer="USA" ism:classification="U">Office of the Director of
      National Intelligence Intelligence Community Chief Information Officer</xhtml:p>
         </xsd:documentation>
      </xsd:annotation>
      <!-- Import the schema for each "dependent" spec. This schema is only used to generate a SchemaGuide -->


<!-- IRM schema because that is the main spec -->

<xsd:import namespace="urn:us:gov:ic:digitalhazmat" schemaLocation="DHZM.xsd"/>

      <!-- TDF schema because an DHZM.XML goes inside a DHZMC-TDO -->

<xsd:import namespace="urn:us:gov:ic:tdf"
                  schemaLocation="../DHZMC-TDF/DHZMC-TDF.xsd"/>
   </xsd:schema>
```