Prepared for:
Department of Homeland Security

Methodology for Developing NIEM Cyber Domain Content

December 1, 2021

Version 1.0

This document is a product of the Homeland Security Systems Engineering and Development Institute (HSSEDI™).

HSSEDI

Homeland Security Systems Engineering & Development Institute™

Homeland Security Systems Engineering & Development Institute

The Homeland Security Systems Engineering & Development Institute (HSSEDI) is a federally funded research and development center (FFRDC) established by the Secretary of Homeland Security under Section 305 of the Homeland Security Act of 2002. The MITRE Corporation operates HSSEDI under the Department of Homeland Security (DHS) contract number 70RSAT20D00000001.

HSSEDI's mission is to assist the Secretary of Homeland Security, the Under Secretary for Science and Technology, and the DHS operating elements in addressing national homeland security system development issues where technical and systems engineering expertise is required. HSSEDI also consults with other government agencies, nongovernmental organizations, institutions of higher education, and nonprofit organizations. HSSEDI delivers independent and objective analyses and advice to support systems development, decision making, alternative approaches, and new insight into significant acquisition issues. HSSEDI's research is undertaken by mutual consent with DHS and is organized by tasks.

This report presents the results of the development of the National Information Exchange Model (NIEM) cyber domain conducted under 43206005-2A: Data Governance and Management.

The information presented in this report does not necessarily reflect official DHS opinion or policy.

This document was prepared for authorized distribution only. It has not been approved for public release.

For more information about this publication contact:

Homeland Security Systems Engineering & Development Institute

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Email: HSSEDI_info@mitre.org

http://www.mitre.org/HSSEDI

Key Words

1. National Information Exchange Model (NIEM)
2. NIEM Cyber Domain
3. NIEM Naming Conventions
4. Cyber Incident Reporting

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

1	3/2/2021		A	Draft release
2	12/1/2021		M	Final release

Table of Contents

List of Figures

This page intentionally left blank

1 Introduction

The release of the new National Information Exchange Model (NIEM) Cyber domain is an opportunity to establish the foundation to enable the receipt and sharing of cyber incident reporting data via standardized information exchanges. This foundation includes:

- Types, elements, and codelists (facets) for incident and breach-related data
- Additional structures to support concepts from the Structured Threat Information Expression (STIX) standard

2 Overview of the methodology for developing the NIEM Cyber domain content

Figure 1 shows an overview of the process for developing the NIEM Cyber domain content. The subsequent sections provide additional information on each of these steps.

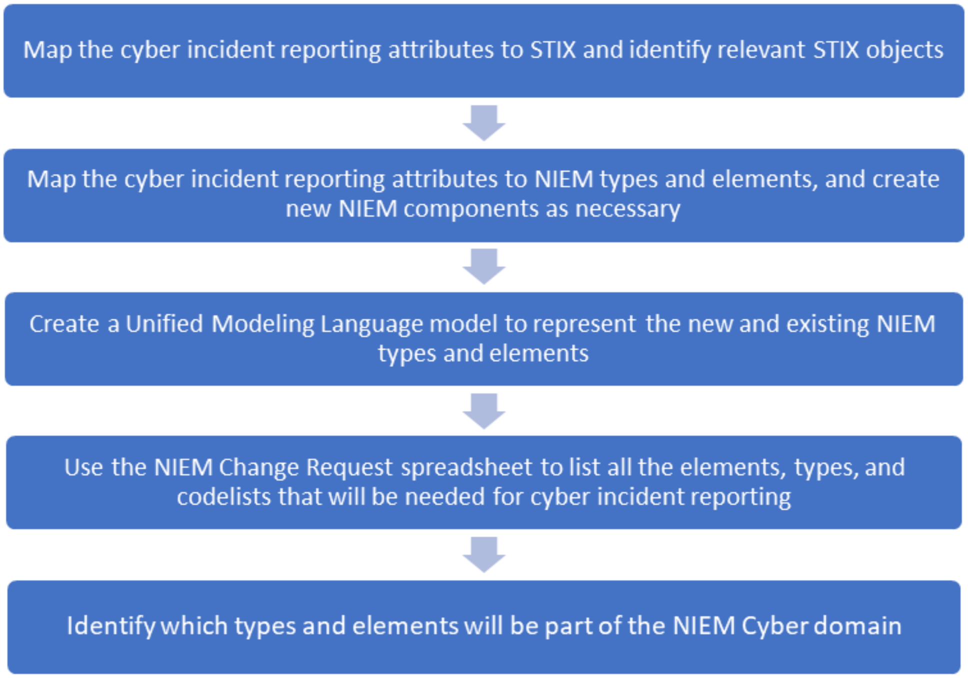
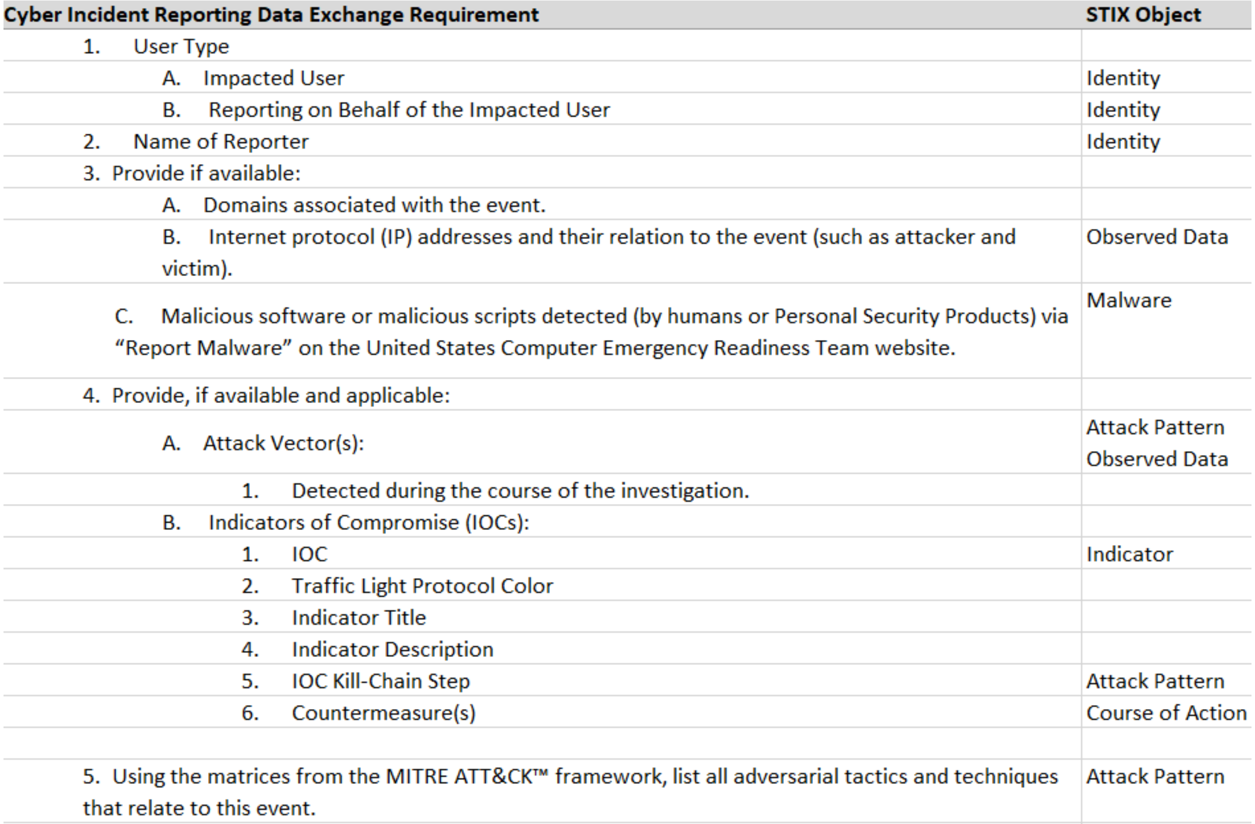

Map the cyber incident reporting attributes to STIX and identify relevant STIX objects
Map the cyber incident reporting attributes to NIEM types and elements, and create new NIEM components as necessary
Create a Unified Modeling Language model to represent the new and existing NIEM types and elements
Use the NIEM Change Request spreadsheet to list all the elements, types, and codelists that will be needed for cyber incident reporting
Identify which types and elements will be part of the NIEM Cyber domain

Figure 1. Overview of the methodology for developing the NIEM Cyber domain content

2.1 Map the cyber incident reporting attributes to STIX and identify relevant STIX objects

Map the cyber incident reporting data exchange requirements to STIX and identify relevant STIX objects. Figure 2 shows a snapshot of the mapping spreadsheet.



Cyber Incident Reporting Data Exchange Requirement	STIX Object
1. User Type	
A. Impacted User	Identity
B. Reporting on Behalf of the Impacted User	Identity
2. Name of Reporter	Identity
3. Provide if available:	
A. Domains associated with the event.	
B. Internet protocol (IP) addresses and their relation to the event (such as attacker and victim).	Observed Data
C. Malicious software or malicious scripts detected (by humans or Personal Security Products) via “Report Malware” on the United States Computer Emergency Readiness Team website.	Malware
4. Provide, if available and applicable:	
A. Attack Vector(s):	Attack Pattern Observed Data
1. Detected during the course of the investigation.	
B. Indicators of Compromise (IOCs):	
1. IOC	Indicator
2. Traffic Light Protocol Color	
3. Indicator Title	
4. Indicator Description	
5. IOC Kill-Chain Step	Attack Pattern
6. Countermeasure(s)	Course of Action
5. Using the matrices from the MITRE ATT&CK™ framework, list all adversarial tactics and techniques that relate to this event.	Attack Pattern

Figure 2. Cyber Incident Reporting Attributes to STIX Objects Mapping Spreadsheet

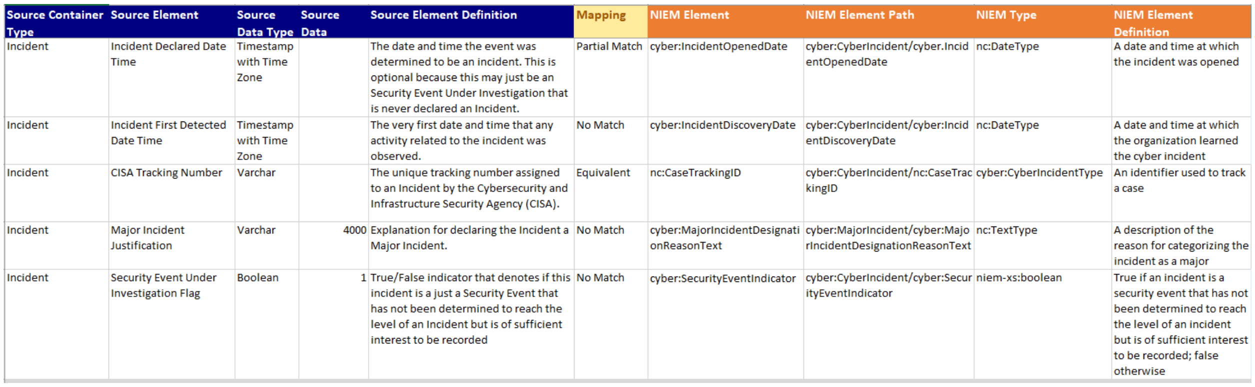
2.2 Map the cyber incident reporting attributes to NIEM types and elements, and create new NIEM components as necessary

The mapping spreadsheet (Figure 3) is intended to be used to facilitate and document the mapping of data sources to NIEM. Mapping is the process of identifying and characterizing similarities between exchange data objects and the NIEM data objects.

Map the cyber incident reporting data exchange requirements to NIEM types and elements, using the following process.

1. If possible, use existing NIEM types and elements. Use the Schema Central tool (http://www.datypic.com/sc/niem41/ss.html) or the NIEM Movement tool (https://beta.movement.niem.gov/#/) to identify existing NIEM elements that can be reused.
2. If a NIEM element exists for a concept for which there is also a relevant STIX object, determine which one to use.
3. Define new equivalent NIEM types and elements for relevant STIX objects.

4. If existing NIEM elements cannot be used, create new types and elements.
5. Define codelists (facets) for the relevant NIEM elements.



Source Container Type	Source Element	Source Data Type	Source Data	Source Element Definition	Mapping	NIEM Element	NIEM Element Path	NIEM Type	NIEM Element Definition
Incident	Incident Declared Date Time	Timestamp with Time Zone		The date and time the event was determined to be an incident. This is optional because this may just be an Security Event Under Investigation that is never declared an Incident.	Partial Match	cyber:IncidentOpenedDate	cyber:CyberIncident/cyber.IncidentOpenedDate	nc:DateType	A date and time at which the incident was opened
Incident	Incident First Detected Date Time	Timestamp with Time Zone		The very first date and time that any activity related to the incident was observed.	No Match	cyber:IncidentDiscoveryDate	cyber:CyberIncident/cyber:IncidentDiscoveryDate	nc:DateType	A date and time at which the organization learned the cyber incident
Incident	CISA Tracking Number	Varchar		The unique tracking number assigned to an Incident by the Cybersecurity and Infrastructure Security Agency (CISA).	Equivalent	nc:CaseTrackingID	cyber:CyberIncident/nc:CaseTrackingID	cyber:CyberIncidentType	An identifier used to track a case
Incident	Major Incident Justification	Varchar	4000	Explanation for declaring the Incident a Major Incident.	No Match	cyber:MajorIncidentDesignationReasonText	cyber:MajorIncident/cyber:MajorIncidentDesignationReasonText	nc:TextType	A description of the reason for categorizing the incident as a major
Incident	Security Event Under Investigation Flag	Boolean	1	True/False indicator that denotes if this incident is a just a Security Event that has not been determined to reach the level of an Incident but is of sufficient interest to be recorded	No Match	cyber:SecurityEventIndicator	cyber:CyberIncident/cyber:SecurityEventIndicator	niem-xs:boolean	True if an incident is a security event that has not been determined to reach the level of an incident but is of sufficient interest to be recorded; false otherwise

Figure 3. Cyber Incident Reporting Attributes to NIEM Elements Mapping Spreadsheet

Overview of the columns in the mapping spreadsheet (Figure 4).

- **Source Container Type:** Cyber incident reporting entity name.
- **Source Element:** Cyber incident reporting attribute name.
- **Source Data Type:** Data type of the cyber incident reporting attribute.
- **Source Data Length:** Data length of the cyber incident reporting attribute.
- **Source Element Definition:** Definition of the cyber incident reporting attribute.
- **Mapping:** Identifies how the source class or element maps to the NIEM class or element using the following mapping categories.
    - Equivalent: Semantics and structure map appropriately. The NIEM element name and definition do not have to be the same as the source element name and definition, but they should have exactly the same conceptual meaning.
    - Partial Match: The element and its semantics or structure only partially match. Otherwise, there are no mismatches or conflicts.
    - No Match: No NIEM element or type maps to the source requirement.
- **NIEM Element:** The name of the NIEM element the source element is mapped to. This field should be an existing NIEM element if an appropriate mapping exists, otherwise a new NIEM element with a name that conforms to the NIEM Naming and Design Rules (NDR) is created.
- **NIEM Element Path:** The path of the NIEM Element within the NIEM Model. The purpose of this element is to allow for traceability back to the element's exact placement in

the NIEM model. Since elements are defined globally, they are shared among containers/types.

- **NIEM Type:** The name of the type being mapped to. This field should be an existing NIEM type of the NIEM element if an appropriate mapping exists, otherwise a new NIEM type with a name that conforms to the NIEM NDR is created.
- **NIEM Element Definition:** The definition of the existing NIEM element if an appropriate mapping exists, or new NIEM element that conforms with the NIEM NDR.

2.3 Create a UML model to represent the new and existing NIEM types and elements

After completing the mapping of the cyber incident reporting attributes to the NIEM elements, create a UML model to represent the elements and the relationship between them. A best practice is to create a new type when there are multiple elements related to a concept. For example, the *CyberIncidentType* is a container for incident related elements such as *MajorIncident*, *IncidentDiscoveryMethod*, *IncidentSeverity*, *AttackPattern*, *Indicator*, *Malware*, etc.

Figure 4 shows a snapshot of an example of the UML model for the NIEM Cyber domain.

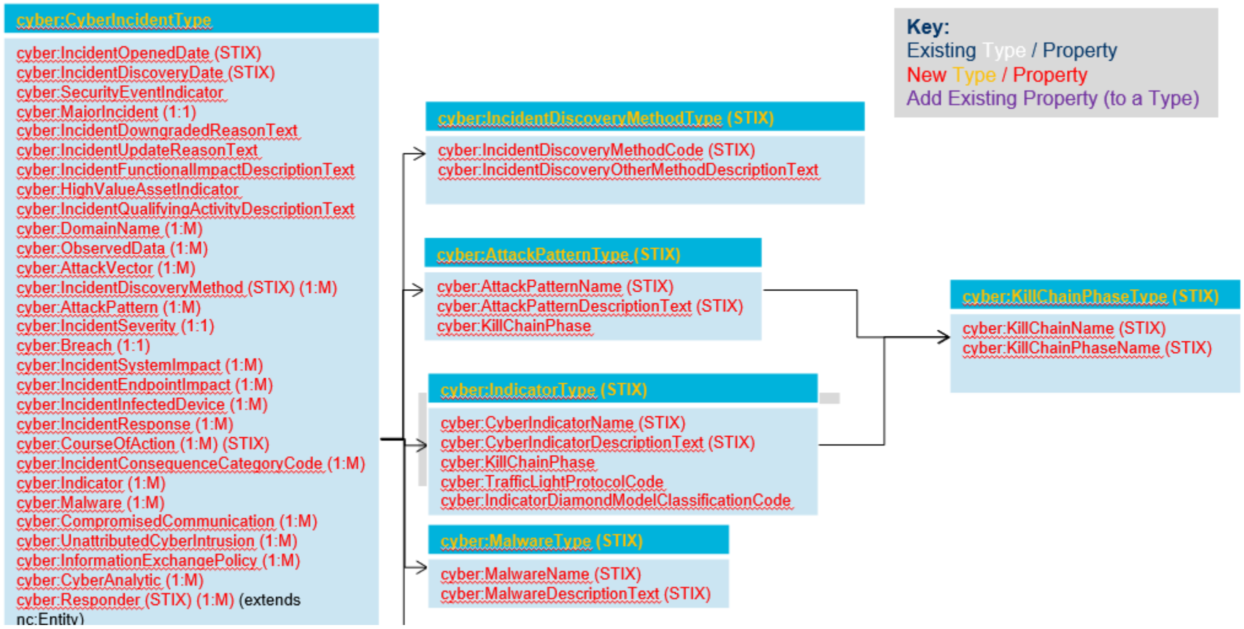

cyber:CyberIncidentType
cyber:IncidentOpenedDate (STIX)
cyber:IncidentDiscoveryDate (STIX)
cyber:SecurityEventIndicator
cyber:MajorIncident (1:1)
cyber:IncidentDowngradedReasonText
cyber:IncidentUpdateReasonText
cyber:IncidentFunctionalImpactDescriptionText
cyber:HighValueAssetIndicator
cyber:IncidentQualifyingActivityDescriptionText
cyber:DomainName (1:M)
cyber:ObservedData (1:M)
cyber:AttackVector (1:M)
cyber:IncidentDiscoveryMethod (STIX) (1:M)
cyber:AttackPattern (1:M)
cyber:IncidentSeverity (1:1)
cyber:Breach (1:1)
cyber:IncidentSystemImpact (1:M)
cyber:IncidentEndpointImpact (1:M)
cyber:IncidentInfectedDevice (1:M)
cyber:IncidentResponse (1:M)
cyber:CourseOfAction (1:M) (STIX)
cyber:IncidentConsequenceCategoryCode (1:M)
cyber:Indicator (1:M)
cyber:Malware (1:M)
cyber:CompromisedCommunication (1:M)
cyber:UnattributedCyberIntrusion (1:M)
cyber:InformationExchangePolicy (1:M)
cyber:CyberAnalytic (1:M)
cyber:Responder (STIX) (1:M) (extends nc:Entity)
cyber:IncidentDiscoveryMethodType (STIX)
cyber:IncidentDiscoveryMethodCode (STIX)
cyber:IncidentDiscoveryOtherMethodDescriptionText
cyber:AttackPatternType (STIX)
cyber:AttackPatternName (STIX)
cyber:AttackPatternDescriptionText (STIX)
cyber:KillChainPhase
cyber:IndicatorType (STIX)
cyber:CyberIndicatorName (STIX)
cyber:CyberIndicatorDescriptionText (STIX)
cyber:KillChainPhase
cyber:TrafficLightProtocolCode
cyber:IndicatorDiamondModelClassificationCode
cyber:MalwareType (STIX)
cyber:MalwareName (STIX)
cyber:MalwareDescriptionText (STIX)
cyber:KillChainPhaseType (STIX)
cyber:KillChainName (STIX)
cyber:KillChainPhaseName (STIX)
Key:
Existing Type / Property
New Type / Property
Add Existing Property (to a Type)

Figure 4. Snapshot of the UML Model for the NIEM Cyber Domain

2.4 Use the NIEM Change Request spreadsheet to list all the elements, types, and codelists that will be needed for cyber incident reporting

After completing the mapping of the cyber incident reporting attributes to NIEM and the UML model for the NIEM Cyber domain, complete the NIEM Change Request spreadsheet.

Remember to revisit the cyber incident reporting attributes to NIEM types/elements mapping spreadsheet, and update for any changes identified in constructing the UML Model.

The Change Request spreadsheet lists all the elements, types and codelists that will be added/edited to the NIEM Cyber domain. The spreadsheet has multiple worksheets:

- **ChangeDescription:** Provides an overview of the changes.
- **Property:** Contains information about the NIEM elements.
  - Change Code: The value will be "Add", since these are new elements.
  - New NS: The namespace prefix of the property. In this case, "cyber" for the NIEM Cyber domain.
  - New Property Name: The name of the property.
  - Definition: The definition of the property.
  - Qualified Data Type: The data type of the property. For complex elements, the value will be the type containing the element, otherwise it will be the actual physical type (e.g. niem-xs:boolean, niem-xs:string, nc:TextType, nc:DateType, etc.).
  - Qualified Substitution Group Head: A property that may be substituted/replaced in XML instances by the property on this row. For example, nc:Entity will be the value of the Qualified Substitution Group Head for the element Responder, as Responder is an extension of nc:Entity.
  - Is Element?: Whether it is an element or attribute. Accepted the default value TRUE, i.e., it is an Element.
- **Type:** Contains information about the NIEM types.
  - Change Code: The value will be "Add", since these are new types.
  - New NS: The namespace prefix of the type.
  - New Type Name: The name of the type.
  - Definition: The definition of the type.
  - Qualified Parent/Base Type: A complex type that has been extended or a simple type that has been restricted by this type.
    - "xs:token" should be the Base Type for all simple types.
    - The Base Type for all CSC types (complex type with simple content) will be the corresponding code simple types. For example, the Base Type for *AttackVectorCategoryCodeType* will be *AttackVectorCategoryCodeSimpleType*.
  - Content Style:
    - "CCC" - Complex type with complex content. These types can carry sub-elements and attributes. This is the default is no value is specified.

        - "CSC" - Complex type with simple content. These types can carry a value and attributes.
        - "S" - Simple type. These types can only carry a value.
    - Is Association: True if the type is an association; false if it is not.
    - Is Augmentation: True if the type is an augmentation; false if it is not.
- **TypeContainsProperty:** Contains information about the NIEM types, and the elements that belong to that type.
    - Change Code: The value will be "Add", since these are new type/element pairs.
    - New Qualified Type: The name of the type in which the property appears as a sub-element or attribute.
    - New Qualified Property: The qualified name (includes namespace prefix) of the property contained in the above type.
    - MinOccurs: The minimum number of times the property may appear under the type. Accepted the element default value, 0.
    - MaxOccurs: The maximum number of times the property may appear under the type. Accepted the element default value, unbounded.
- **Facet:** Contains information about the codelists.
    - Change Code: The value will be "Add", since these are new codelists.
    - New Qualified Type: The name of the type. Use "stix" as namespace for codelist taken directly from STIX.
    - New Facet Value: A code value or other kind of value of the facet.
    - Definition: The definition of the facet.
    - Kind of Facet (default=enumeration): Usually an enumeration; this could also be other kinds of facets, such as minInclusive, maxExclusive, pattern, and so forth. Accepted the default value, enumeration.

2.5 Identify which types and elements will be part of the NIEM Cyber domain

Not all the elements will be part of the NIEM Cyber domain. There are some elements that will be used only for cyber incident reporting; these will be part of the cyber incident reporting-specific Information Exchange Package Documentation (IEPD). If there is expected reuse by another stakeholder, the best practice is to include in the NIEM Cyber domain.

3 Best Practices

3.1 Type Naming

- Type names should begin with the class term. For example, instead of naming the type as *EndpointImpactType*, the type name should be *IncidentEndpointImpactType*.
- Type names should end with the suffix "type". For example, *AttackPatternType*, *BreachType.*
- Types with a name that ends in "CodeType" should correspond to a code set. For example, *AttackVectorCategoryCodeType* will have a corresponding codelist (facet) that specifies permissible values.
- "xs:token" is usually the Base Type for all simple types. For example, the Base Type for *BreachNotificationMethodCodeSimpleType* will be "xs:token".
- The Base Type for all CSC types (complex type with simple content) will be the corresponding code simple types. For example, the Base Type for *AttackVectorCategoryCodeType* will be *AttackVectorCategoryCodeSimpleType*.

3.2 Element Naming

- Element names should begin with the class term. For example, instead of naming the element as *ReportedToCongressDateTime*, the element name should be *CyberIncidentReportedToCongressDateTime.*
- Elements that contain a Boolean value should end with "Indicator". For example, *HighValueAssetIndicator.*
- It a good practice for element names to have a representation term such as Indicator, Name, Text, etc. Having a representation term indicates the nature of the value carried by the element, and labeling elements and attributes with a notional indicator of the content eases discovery and comprehension. For example, *IncidentLogAvailableIndicator, FISMASystemCategoryName, MalwareDescriptionText*.
- For element names that are an extension of an existing NIEM element, the Qualified Substitution Group Head will have the value of the existing NIEM element name. For example, *nc:Entity* will be the value of the Qualified Substitution Group Head for the element *Responder*.

3.3 Data Type

- Represents the data type of the element. For example, if the element was *nc:Person*, the data type would be *nc:PersonType*; if the element was *nc:PersonBirthDate*, the data type would be *nc:DateType*; if the element was *cyber:DomainName*, the data type would be *nc:TextType* or niem-xs:string; if the element was *cyber:BreachIndividualsNotifiedIndicator*, the data type would be niem-xs:boolean.

3.4 Type Definition

- Type names should be defined using the format – "A data type…". For example, the type *BreachNotificationType* will be defined as "A data type for a notification of a breach".

3.5 Element Definition

- The definition of all element names should begin with "A".
- Element names that end with "name" should be defined using the format – "A (optional adjective) name ... ". For example, the element *ProtocolName* will be defined as "A name of a network protocol used for communication".
- Element names that have the word "CategoryCode" in their name, such as *PIIBreachCategoryCode*, *IncidentConsequenceCategoryCode* should be defined using the format – "A kind of ... " or "A statement of …". For example, the element name *IncidentConsequenceCategoryCode* will be defined as "A kind of consequence resulting from an incident". *CategoryCodes* usually indicate a corresponding facet to delineate the set of valid values.
- Element names that end with "indicator" should be defined using the format – "True if …; false otherwise|if". For example, the element *BreachIndividualsNotifiedIndicator* will be defined as "True if impacted individuals were notified of a breach; false otherwise".

List of Acronyms

Acronym	Definition
CCC	Complex type with Complex Content
CISA	Cybersecurity and Infrastructure Security Agency
CSC	Complex type with Simple Content
FCEB	Federal Civilian Executive Branch
FING	Federal Incident Notification Guidelines
IEPD	Information Exchange Package Documentation
NDR	Naming and Design Rules
NIEM	National Information Exchange Model
STIX	Structured Threat Information Expression
UML	Unified Modeling Language
XML	Extensible Markup Language

Glossary

Glossary Term	Glossary Definition
Namespace	Namespaces act like collections, logically grouping related properties and types together. Components are often referred to by their qualified names, like *nc:Person*. Using the namespace prefix in front of the component name helps to identify and distinguish it, especially in cases where the same name may appear in multiple namespaces.
Property	A property represents a concept, idea, or thing. It defines specific semantics and appears in exchanges as the tag or label for a field. In NIEM, there are two basic kinds of properties: elements and attributes. • Attributes can only ever be used to represent simple content (a value). They do not exist independently; they must be carried by an element. • Elements can be used to represent simple content (a value) or complex content (an object). In either case, an element can also carry attributes.
Type	A type defines a structure – an allowable set of values. A type might describe a simple value (e.g., a string, a number) or a complex object (e.g., PersonType).
Facet	Facets are additional constraints that may be defined on simple types (like strings or numbers) to limit the allowable values. They can do such things as limit a string to a pre-defined code list, constrain a number to a given range, or create a pattern that must be followed.
Information Exchange Package Documentation	An Information Exchange Package Documentation (IEPD) is a collection of NIEM artifacts. They define and describe the context, content, semantics, and structure of one or more implementable information exchanges.

List of References

1. NIEM Reference, http://niem.github.io/reference/
2. NIEM Model Concepts, http://niem.github.io/reference/concepts/
3. NIEM Movement Tool, https://beta.movement.niem.gov/#/
4. Schema Central Tool, http://www.datypic.com/sc/niem41/ss.html
5. NIEM Naming and Design Rules (NDR) Specification, https://niem.github.io/reference/specifications/ndr/
6. STIX Documentation, https://oasis-open.github.io/cti-documentation/resources.html