NIEM IEPD vs. STIX PROFILE

COMPARISON

**Version 1.2**

**August 02, 2013**

Table of Contents

[1. Introduction 5](#_Toc363228805)

[1.1 NIEM 5](#_Toc363228806)

[1.1.1 NIEM IEPD 5](#_Toc363228807)

[1.2 STIX 5](#_Toc363228808)

[1.2.1 STIX PROFILE 5](#_Toc363228809)

[1.3 STIX PROFILE vs. NIEM IEPD 6](#_Toc363228810)

[1.3.1 Similarities 6](#_Toc363228812)

[1.3.2 Differences 7](#_Toc363228813)

[1.4 CONCLUSION 7](#_Toc363228814)

[1.4.1 Pros and Cons of NIEM IEPD 7](#_Toc363228815)

[1.4.2 Pros and Cons of STIX Profile 8](#_Toc363228816)

[1.4.3 Conclusion 9](#_Toc363228817)

1. Introduction

This document is meant to provide a high-level comparison of the National Information Exchange Model (NIEM) Information Exchange Package Document (IEPD) and the Structured Threat Information Exchange (STIX) Profile, as used in information exchange by NIEM and STIX communities. It is meant to compare and contrast the above mentioned information exchange products and methodologies.

It is important to note that the document is neither meant to endorse nor promote any particular product or methodology, but is rather meant to provide stakeholders and practitioners with a holistic view of the aforementioned products and methodologies, in order to make informed decision when selecting what to use for information exchange.

* 1. NIEM

NIEM is a collaborative information exchange framework used by government (federal, state, tribal, and local) and private industry. Some of the communities actively using NIEM are: *Health and Human Services justice, public safety, homeland security, management, intelligence* and *DoD (recent).*

* + 1. NIEM IEPD

A NIEM IEPD captures information exchange components with additional artifacts, XML Schemas and business rules.

* 1. STIX

STIX is a collaborative effort to define and develop a standardized representation of structured cyber threat information. It brings together stakeholders across government (federal, state, tribal, and local) and private industry.

* + 1. STIX PROFILE

STIX Profile refers to an encoding for cyber threat intelligence use case for sharing cyber threat information within a given community. Even though a STIX profile is a subset of the STIX model, the components may vary based on the scenario.

* 1. STIX PROFILE vs. NIEM IEPD

The tables below have been used to compare and contrast STIX Profile and NIEM IEPD.

* + 1. Similarities

|  |
| --- |
| Similarities between NIEM IEPD and STIX Profile |
| Both consist of human‐readable spreadsheets as a means of representing initial exchange components:   * Profiles are documented and distributed via human‐readable spreadsheets * Initial IEPD components are represented in human‐readable spreadsheets |
| Both have additional accompanying artifacts:   * IEPDs contain additional mandatory and optional exchange documentation such as business documents, MOUs and others that give supplementary information about information exchange * STIX profile contains additional optional documentation detailing aspects of the profile besides the component spreadsheet. The nature of additional documents would vary based on the stakeholder preferences i.e. business documents, technical documents and or guidelines |
| Both have defined conformance guidelines that have to be adhered to:   * The NIEM conformance rules have to be met for an IEPD to be NIEM-conformant * STIX Profile Requirements rules are used to determine whether a given Profile is compliant or not |
| Both have clearly defined development lifecycles:   * There exists a clearly defined, IEPD development process for developing IEPDs * There currently exists a well-defined STIX Profile development process for developing a STIX Profile |

* + 1. Differences

|  |  |
| --- | --- |
| Differences between NIEM IEPD and STIX Profile | |
| NIEM IEPD | STIX PROFILE |
| A NIEM IEPD may or may not have a child or subset IEPD and if it does have one, then the constraints may or may not exist based on the contextual exchange requirement. | STIX Profiles can have child profiles. The Child Profile MUST NOT expand the content or loosen the constraints specified by the parent profile such that instances of documents are compliant with the child but not the parent. |
| A NIEM IEPD is not confined to a specific domain; there can be cross-pollination of exchange components from other domains i.e. a Cyber threat IEPD could re-use components already defined in Intelligence, Justice or other domains. | A STIX Profile is specifically developed for sharing Cyber Security Threat information. This therefore means that other domains cannot use STIX Profiles unless within the context of Cyber Security. |
| External exchange components can be embedded in a NIEM IEPD, as long as they adhere to the NIEM conformance rules. | STIX Profiles cannot add or subtract from STIX. Also, instance documents may not be considered compliant if they comply against the STIX Profile but are not compliant against STIX. |
| Exchange components used in NIEM IEPDs are primarily based on the NIEM Model. | Exchange components used in STIX Profiles are primarily based on the universal STIX Model. |

* 1. CONCLUSION
     1. Pros and Cons of NIEM IEPD

|  |  |
| --- | --- |
| NIEM IEPD | |
| PROS | CONS |
| A NIEM IEPD is not restricted to one domain/subject and can have components from various domains and groups besides cyber i.e. Intelligence, trade and others. | There are no readily available components as the NIEM Cyber components have yet to be defined in the NIEM Model. |
| There is readily available support for NIEM IEPDs through the vibrant stakeholder community i.e. State, local, tribal, federal and international. | There is a steep learning curve for building new expertise in NIEM to carry out IEPD development. |
| A NIEM IEPD contains numerous artifacts with adequate information  relating to information exchange thus making it easier to understand the context at any given point. | The requirement for numerous artifacts in an IEPD can be a hindrance to adoption by various groups who might not like producing and maintaining numerous documents. |
| The presence of NIEM conformance for IEPDs can positively instill discipline in building exchanges. | The presence of NIEM conformance rules could also be a barrier to independent-minded agencies. |
| A NIEM IEPD can be scaled and re-used as need arises which saves cost and effort. | In some unique cases, creating new IEPDs could be cheaper than re-using existing ones. |

* + 1. Pros and Cons of STIX Profile

|  |  |
| --- | --- |
| STIX Profile | |
| PROS | CONS |
| Purely focused on Cyber and as such greater details pertaining to the domain have been defined and refined by the community. | Is relatively new and as such is yet to have strong representation besides initial groups i.e. state, local, tribal, and federal. |
| A STIX Profile provides the flexibility of constraining a segment of the STIX model to a given exchange context. | The stringent profile rules could be a barrier to flexibility for a given exchange context. |
| Provides a clear scope for tool/service implementation capability. | Reaching a consensus on scope for tool/service implementation can be a lengthy process at times. |
| Different Profiles can be created as subsets of others (layering), hence reusability which saves time and effort. | The stringent conformant rules for creating new Profiles though layering could be a barrier to new implementers. |

* + 1. Conclusion

From the above, we can see that even though a STIX Profile has similarities to a NIEM IEPD, they also have some differences. This therefore means that while making a selection on which one between the two to use, it is pertinent that further consideration ought to be given to additional prevailing factors existing in an information exchange context.