15 July 2010

Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Presentation**
In the Matter of: Cyber Security Certification Program, Docket No. PS 10-93

Dear Ms. Dortch:

This is to inform you that Anthony M. Rutkowski, EVP for Regulatory Affairs and Standards of Yaana Technologies LLC, engaged in eMail communication on 13 July with Jeffrey Goldthorp, Chief, Communications Systems Analysis Division, and Gregory Intoccia, Cybersecurity Legal Counsel of the Public Safety and Homeland Security Bureau.

The purpose of this communication was to provide a recently revised copy of the principal emerging global cyber security information exchange framework specification, X.cybex (X.1500). As described in Yaana Technologies Comments, the broad global industry effort to advance this specification has a significant potential relationship to the issues raised in the *Cyber Security Certification Program Notice of Inquiry*.

Mr. Rutkowski also expressed the view to the staff that the Comments filed in the proceeding were few, and seem to reflect a kind of typical Washington "knee-jerk" reaction to the Commission's scaling a long-overdue role through this proceeding; and that the staff deserves praise for the thoughtful and innovative work manifested in the NOI. He encouraged continued focused Commission actions along the lines outlined in Yaana's Comments.

This submission reflects the communication that occurred.

Although Mr. Rutkowski is also the ITU-T Cybersecurity Rapporteur within whose Group the CYBEX initiative is occurring, he was expressly not representing the views of that international Group in the context of this communication or the 10-93 proceeding, as implementation of ITU-T Recommendations is regarded as a national matter.

Pursuant to the Commission's rules, this *ex parte* letter is being filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

/s/

Anthony M. Rutkowski
SVP for Regulatory Affairs and Standards
Yaana Technologies, LLC
500 Yosemite Drive, Suite 120
Milpitas, CA 95035
tel: +1 408.854.8041
mailto:tony@yaanatech.com

Attachment: **Draft Rec. ITU-T X.cybex (X.1500)**

X.cybex

Recommendation ITU-T X.cybex
Cybersecurity information exchange framework

Summary

This Recommendation.

a) establishes a framework and general principles for coherent, comprehensive, global, timely and assured exchange of cybersecurity information

b) enables this exchange by
- identifying and incorporating existing standards implemented in various environments
- as necessary, making the existing standards more global and interoperable
- providing extensible means for adapting to new exchange requirements and capabilities

As a result of implementing this Recommendation, telecommunication/ICT organizations, including Computer Incident Response Teams (CIRTs), both within and between jurisdictions, will:

a) have information to enable decision making and action to substantially enhance the confidentiality, integrity and availability of global telecommunication/ICT facilities and services;

b) have adopted secure collaborative processes and controls, including those for Secure Online Transactions, which raises the assurance between organizations exchanging the information as well as the assurance of that information;

c) be using a coherent approach to manage and exchange cybersecurity information on a global basis;

d) improve security awareness and collaboration.

Objective

The Recommendation objective is assured cybersecurity information exchange. It moves beyond guidelines and facilitates the scaling and broad implementation, of core assurance, operational risk management, and response capabilities – many of which have already been developed within existing insular cybersecurity communities. The framework also takes into consideration emerging cloud computing environments, and can be easily applied to new applications such as SmartGrid and eHealth cybersecurity.

The Recommendation provides for this objective via a framework that allows for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums, and consists of a basic exchange framework with the following extensible functions:

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- requesting and responding with cybersecurity information
- exchanging cybersecurity information over networks
- assured cybersecurity information exchanges

The Recommendation describes ways in which a common understanding can be reached to enable assured exchange of information for responding to incidents and potentially reducing the risk and exposure caused by vulnerabilities.

These functions are organized into several exchange “clusters” :

- Weakness, vulnerability, state exchange
- Event, incident, heuristics exchange
- Exchange of policies
- Evidence exchange
- Cybersecurity heuristics and information request
- Cybersecurity entity identification and discovery
- Cybersecurity assured exchange

A compendium of many related recommendations, guidelines and practices is included in Appendix B for reference.

X.cybex

Candidate Recommendation ITU-T X.cybex

Cybersecurity Information Exchange Framework

Table of Contents

1. Scope 5
2. References 5
3. Definitions 5
   3.1 Terms defined elsewhere 5
   3.2 Terms defined in this Recommendation 5
4. Abbreviations and acronyms 6
5. Conventions 7
6. Basic concept of the Cybersecurity Information Exchange Framework 7
   6.1 Description of the Framework 7
   6.2 Description of the context of the framework 8
   6.3 Cybersecurity Information Exchange Framework Ontology 9
      6.3.1 Operation Domains 10
      6.3.2 Cybersecurity Entities 10
      6.3.3 Cybersecurity Operational Information 10
7. Cybersecurity structured information 13
   7.1 Weakness, Vulnerability and State Exchange Cluster 14
   7.2 Event, Incident, Heuristics Exchange Cluster 16
   7.3 CIRT Policy Exchange Cluster 17
   7.4 Evidence Exchange Cluster 17
   7.5 Cybersecurity Heuristics and Information Request Cluster 18
   7.6 Relationships and dependencies among cybersecurity structured information specifications and derivative extensions 18
   7.7 Cybersecurity entity identification and discovery 20
   7.8 Common Cybersecurity Identifier (CCI) 20
8. Cybersecurity assured exchange 21
   8.1 Assurance of Identities 21
   8.2 Information Exchange Protocols 21

Appendix A – Security Automation Schema Use Cases 23

Appendix B: compendium of cybersecurity requirements and guidelines 24

History

Sep 2009. Initial draft (including TSB Director-SG17chair editorial change of CYBIEF to CYBEX)
Apr 2010 SG17 Meeting revision

RECOMMENDATION ITU-T X.cybex

Cybersecurity Information Exchange Framework

1. Scope

This Recommendation facilitates coherent, comprehensive, global, timely, and assured exchange of cybersecurity information. It includes the structured global discovery and interoperability of that information in a framework that allows for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cybersecurity forums, including cloud computing, and new applications such as SmartGrid and eHealth cybersecurity.

The scope of the framework includes an information exchange model that currently has the following basic functions that can be used separately or together as appropriate, and extended as needed.

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- requesting and responding with cybersecurity information
- exchanging cybersecurity information over networks
- assured cybersecurity information exchanges

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T A.1] ITU-T Recommendation A.1 (2006), *Work methods for study groups of the ITU Telecommunication Standardization Sector (ITU-T).*

[ITU-T A.5] ITU-T Recommendation A.5 (2001), Generic procedures for including references to documents of other organizations in ITU-T Recommendations.

3. Definitions

3.1 Terms defined elsewhere

3.2 Terms defined in this Recommendation

3.2.1 Cybersecurity entity: any entity that is part of an exchange of cybersecurity information, including the information object itself.

3.2.2 Computer Incident Response Team: An organization or team that may provide services and support to a defined constituency for preventing, handling, and responding to computer or computer-assisted security incidents.

3.2.3 Cybersecurity information: structured information or knowledge concerning:

1. The "state" of equipment, software, or network based systems as related to cybersecurity, especially vulnerabilities
2. Forensics related to incidents or events
3. Heuristics and signatures gained from experienced events
4. Cybersecurity entities involved
5. Specifications for the exchange of cybersecurity information, including modules, schemas, terms & conditions, and assigned numbers
6. The identities and assurance attributes of all cybersecurity information
7. Implementation requirements, guidelines and practices

3.2.4 Cybersecurity Operations: Methods and processes used to monitor and manage security within defined operational limits including:

- The collection and analysis of behavioral information which may have an effect on security.
- The detection of behavior which adversely effects security or by which the likelihood of a future adverse effect can be determined.
- Action taken in the event of an adverse behavior taking place in order to limit, mitigate and/or prevent future occurrences of the adverse behavior or its effects.
- Security-related communications, whether physical, virtual or otherwise network related concerning the status and condition of systems.

3.2.5 Exchange Protocol: A set of technical rules and associated behavior governing the exchange of information between two or more computer systems via a network.

3.2.6 Incident: a set of events that have been determined (through machine or human interpretation) to have caused or is intended to cause harm.

3.2.7 Policy: Terms and conditions associated with the use and sharing of cybersecurity information

3.2.8 State: the current status of a system or entity, including such information as its configuration, memory usage, or other data relevant to cybersecurity.

4. Abbreviations and acronyms

ARF Assessment Result Format

BEEP Blocks Extensible Exchange Protocol

CAPEC Common Attack Pattern Enumeration and Classification

CCE Common Configuration Enumeration

CEE Common Event Expression

CEEE Common Event Expression Exchange

CERT Computer Emergency Response Team

CYIQL Cybersecurity Information Query Language

CPE Common Platform Enumeration

CIRT Computer Incident Response Team

CVE Common Vulnerabilities and Exposures

CVSS Common Vulnerability Scoring System

CWE Common Weakness Enumeration

CWSS Common Weakness Scoring System

DEXF Digital Evidence Exchange Format

EDRM Electronic Discovery Reference Model

EVCERT Extended Validation Certificate Framework

ICT Information and Communications Technology

IODEF Incident Object Description Exchange Format

LEA Law Enforcement Agency

MAEC Malware Attribute Enumeration and Characterization

OVAL Open Vulnerability and Assessment Language

SCAP Security Content Automation Protocol

SOAP Simple Object Access Protocol

XCCDF eXensible Configuration Checklist Description Format

5. Conventions

None

6. Basic concept of the Cybersecurity Information Exchange Framework

6.1 Description of the Framework

The Cybersecurity Information Exchange Framework (CYBEX) is intended to accomplish a simple, limited objective – namely a common global means for cybersecurity entities to exchange cybersecurity information – generally over a network of some kind. Such entities typically consist of organizations, persons, objects, or processes possessing or seeking cybersecurity information. Most frequently, these entities are CIRTs and the operators or vendors of equipment, software or network based systems.

The cybersecurity information exchanged is valuable for achieving enhanced cybersecurity and infrastructure protection, as well as accomplishing the principal functions performed by CIRTs.

The exchange of cybersecurity information typically occurs within highly compartmentalized trust communities until remedies are devised and available. At such time, knowledge of the threats, vulnerabilities, incidents, risks, and mitigations and the associated remedies are made public. The related specifications included in this framework are intended to facilitate these processes and thereby enhance cybersecurity. Ref. ITU-T Rec. X.1206.

This exchange process is depicted below in Figure 1 as consisting of the following functions:

- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- requesting and responding with cybersecurity information
- exchanging cybersecurity information over networks
- assured cybersecurity information exchanges

Sections 7 through 8 of this Recommendation set forth specifications for accomplishing these functions.

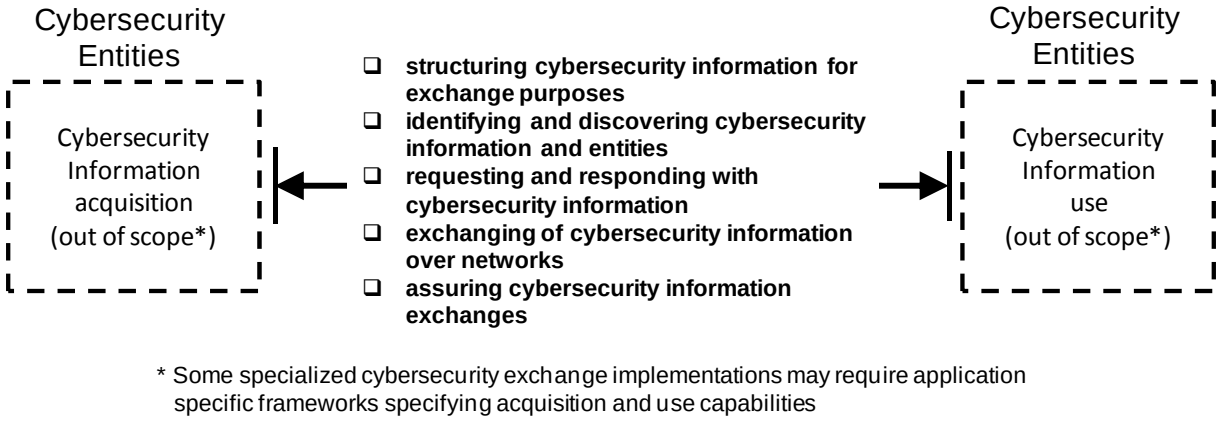

Figure 1 – Framework for the exchange of cybersecurity information

The exchange framework is bi-directional. This bi-directionality allows for both information requests and verified responses to facilitate required levels of assurance between the parties or provide certification of delivery.

Subject to agreed policies, the means of acquiring information as well as the uses made of the information are generally out of scope and not treated in this Recommendation. However, some specialized cybersecurity exchange implementations such as traceback of attack sources may require application specific frameworks specifying acquisition and use capabilities specific to that kind of exchanged information and allow for a recursive series of requests and responses to obtain required information. Such implementations also include making cybersecurity measureable, for example, through the use of security content automation protocols.

This framework applies to the formats and mechanisms for the exchange of this information and does not mandate in any way the exchange of cybersecurity information.

6.2 Description of the context of the framework

Although specific acquisitions and uses are out of scope, it is useful at the macro level to describe the implementation context of the Framework. The Framework enables exchange capabilities, by supporting the dashed exchanges in the illustrative example shown in Figure 2, below. This example portrays a coherent set of capabilities that include measures to facilitate protection, threat detection, thwarting and patching, and legal remedies through the trusted exchange of cybersecurity information. Necessary cybersecurity information exchange is indicated with dashed lines with arrows. In Figure 2, CIRT activities typically encompass all the measures that enable:
1) threat detection and 2) thwarting or other remedies.

The Framework is also equally applicable when the components are highly distributed, or integrated in the form of Cloud Computing.

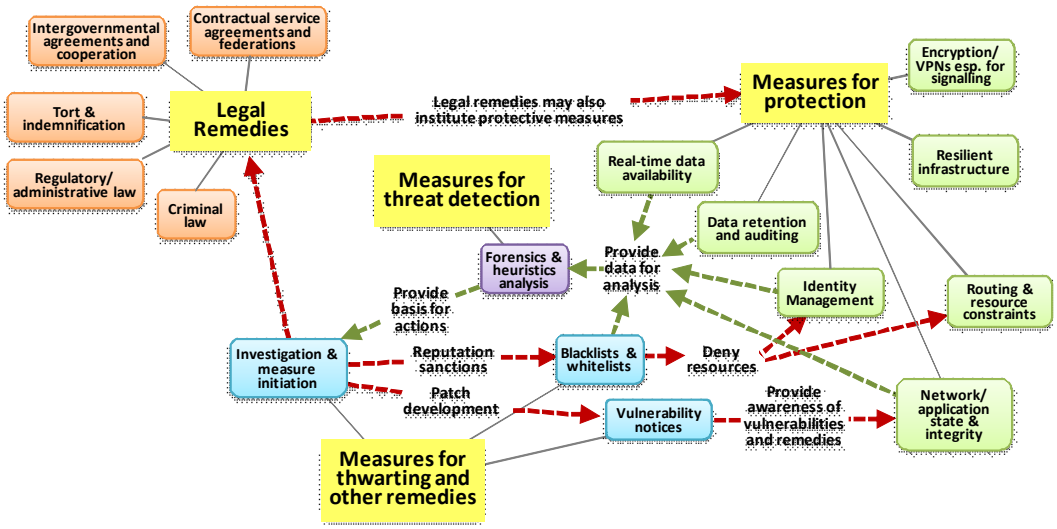

Figure 2 – The Cybersecurity illustrative example supported by the exchange of cybersecurity information

6.3 Cybersecurity Information Exchange Framework Ontology

The cybersecurity capabilities depicted in Figure 2 above are usefully described within a CYBEX ontology; that is, a model for describing the acquisition, accumulation and use of cybersecurity information knowledge that consists of a set of types, properties, and relationships. See Figure 3. The solid lines describe the relationship of the information types, while arrows describe information input from an entity to knowledge base/database. The functions shown on the right are generic and entities such as ISRTs, may encompass one or more of these functions.

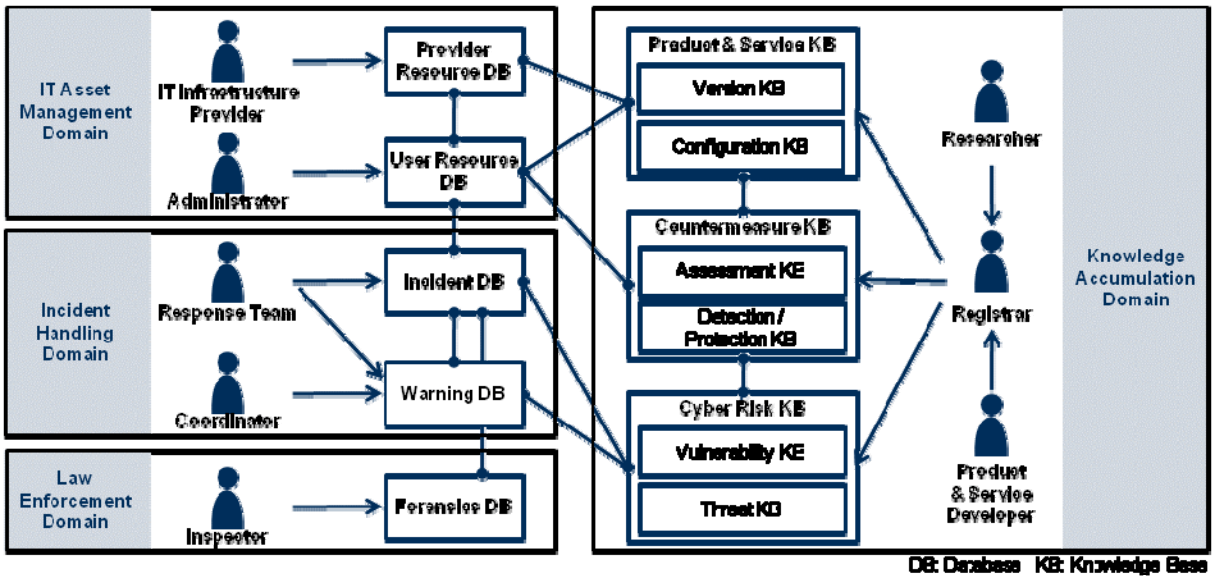

Figure 3 - Model for the CYBEX ontology

This model is used to define domains for cybersecurity operations, which is then used to identify required cybersecurity entities to support the operations in each domain. A detailed ontology is then derived. The CYBEX framework of specifications supports this ontology.

6.3.1 Operation Domains

Cybersecurity operations principally consist of three domains: Incident Handling, ICT Asset Management and Knowledge Accumulation.

The Incident Handling Domain includes detection and response to cybersecurity incidents by monitoring incidents, computer events that constitute the incidents, and attack behavior caused by the incidents. For instance, it detects abnormalities through alarms from detectors, and then builds enumerations by collecting various logs. Sometimes it provides alerts and advisories, e.g. early warnings against candidate threats, to user organizations.

ICT Asset Management Domain includes cybersecurity operations within each user organization such as installing, configuring, and managing ICT assets in the organization. It includes both incident preventive operations and damage controlling operations in each organization.

The Knowledge Accumulation Domain includes cybersecurity-related information research. Reusable knowledge for other organizations is generated and accumulated.

6.3.2 Cybersecurity Entities

Based on the operation domains described above, the cybersecurity entities that are necessary to run cybersecurity operations in each domain can be identified.

Within the Incident Handling Domain, two entities exist for its operations; the Response Team, and the Coordinator. The Response Team is an entity that monitors and analyzes various kinds of incidents, e.g. unauthorized access, DDoS attack and phishing, and accumulates incident information. Based on this information, a Response Team may implement countermeasures, e.g. register phishing site addresses on black lists. A Coordinator is an entity that coordinates with the other entities and addresses potential threats based on known incident and crime information.

In the IT Asset Management Domain, two operation entities exist: Administrator and IT Infrastructure Provider. The Administrator administers the system of its organization and possesses information on its own IT assets. An IT administrator inside each organization is its typical instance. The IT Infrastructure Provider provides each organization with IT infrastructures, which includes the network connectivity, cloud services such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), and identity. An Internet Service Provider (ISP) and Application Service Provider (ASP) are its typical instances.

In the Knowledge Accumulation Domain, three operation entities exist: Researcher, Product & Service Developer and Registrar. A Researcher researches cybersecurity, extracting and accumulating knowledge. A Product & Service Developer possesses information on products and services, e.g. naming, versions, their vulnerabilities, their patches and configuration information. A software vendor, ASP and individual software programmers are typical instances. A Registrar is an entity that classifies and organizes cybersecurity knowledge provided by Researcher and Vendor so that the knowledge can be used for another organization.

6.3.3 Cybersecurity Operational Information

Based on the operation domains and entities, this section elaborates cybersecurity operational information provided by the entities for each operation domain.

6.3.3.1 Incident Handling Domain

In the Incident Handling Domain, there exists Incident Database and Warning Databases. An Incident Database contains information on incidents provided by a Response Team. It includes three kinds of records: Event, Incident, and Attack. An Event Record includes computer events such as root user's logging into a system. It also includes information on packets, files and their

transactions. Usually, most of the records are provided by computers automatically. An Incident Record includes events that are incident candidates. This record is usually derived from several Event Records and their conjectures, which are created automatically and/or manually. An Attack Record is based on the analyses of incidents and includes the precise date and time of the attacks as well as their sequences.

A Warning Database includes information on cybersecurity warnings provided by Response Team and Coordinator. The warnings are based on the Incident Database as well as Cyber Risk Knowledge Base.

6.3.3.2 ICT Asset Management Domain

In the ICT Asset Management Domain, there exists two databases: User Resource Database and Provider Resource Database.

The User Resource Database accumulates information on assets inside individual organization and contains information such as the list of software, hardware, their configurations, status of resource usage, security policies including access control policies, security level assessment result, and intranet topology. The information is provided by the Administrator.

The Provider Resource Database accumulates information on assets outside individual organization. It mainly contains external resource information and external network information. External resource information contains information on resources that each organization is utilizing outside their organization such as the list and status of external cloud services (e.g., data center and SaaS). The External network information contains information on networks with which each organization is connected with the other organizations such as their topology, routing information, access control policy, traffic status and the security level. The information is provided by the IT Infrastructure provider.

6.3.3.3 Knowledge Accumulation Domain

Three knowledge bases exist in the Knowledge Accumulation Domain: for Cyber Risks, Countermeasures, and Products. They accumulate knowledge on cybersecurity provided by Researcher and Product & Service Developer, which is then organized and classified by the Registrar.

The Cyber Risk Knowledge Base accumulates cybersecurity risk information and includes Vulnerability Knowledge and Threat Knowledge. The Vulnerability Knowledge Base accumulates known vulnerability information, including naming, taxonomy and enumeration of known vulnerability information. It also includes human vulnerabilities exposed by human IT users. The Threat Knowledge Base accumulates known threat information that includes Attack Knowledge and Misuse Knowledge. The Attack Knowledge is on attacks including information on attack patterns, attack tools (e.g. malware) and their trends such as the information on past attack trends in terms of geography and attack target. It also includes statistical information of past attacks. The Misuse Knowledge is on misuses caused by human users without any malicious intention. Information of mistyping, being caught by phishing traps, and compliance violations are included.

The Countermeasure Knowledge Base accumulates information on countermeasures to cybersecurity risks and contains two knowledge bases: Assessment and Detection/Protection The Assessment Knowledge Base accumulates known rules and criteria for assessing security level of IT assets as well as the checklist of configurations. The Detection/Protection Knowledge Base accumulates known rules and criteria for detecting/protecting security threats, for example IDS/IPS signatures and related detection/protection rules.

The Product & Service Knowledge Base accumulates information on products and services. It includes two knowledge bases: Version Knowledge and Configuration Knowledge. The Version

Knowledge Base accumulates version information on products and services, including naming and enumeration of their versions. Regarding product version, security patches are also included within the knowledge base. The Configuration Knowledge Base accumulates configuration information on products and services. Regarding product configuration, it includes naming, taxonomy and enumeration of known configurations.

Each of the databases and knowledge bases mentioned above may utilize various information description standards as shown in Figure 4.

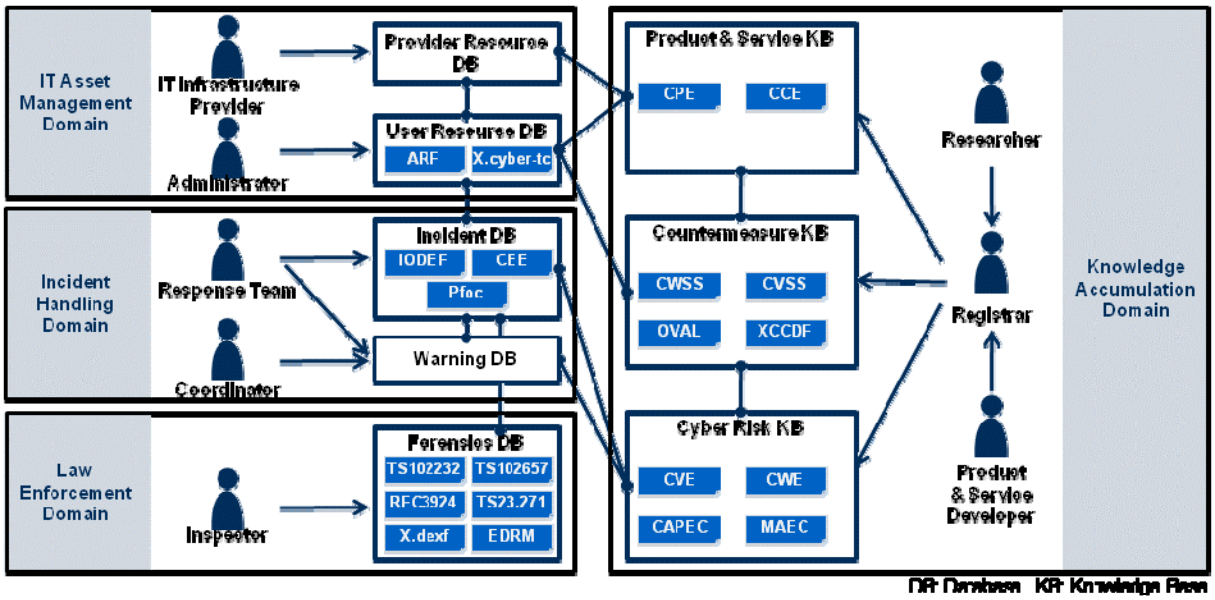

Figure 4 - Detailed view of the CYBEX ontology

A mapping between this ontology and the cybersecurity structured information specifications described in Sec. 7 is provided in Sec. 7.6, below.

7. Cybersecurity structured information

For the exchange of cybersecurity information to occur as messages between any two entities, it must be structured and described in some consistent manner that is understood by both of those entities. This section describes specifications that enable this exchange. The goal is to make it easier to share cybersecurity information that often includes "common enumerations," that is, ordered lists of well-established information values for the same data type. Common enumeration allows distributed databases and other capabilities to be linked together, and to facilitate cybersecurity related comparisons. Subsequent sections of this Recommendation treat other essential parts of the framework such as cybersecurity identification, discovery, and assured exchange.

Some existing specifications are simply identified; while others are being imported as X-series specifications. The choice of treatment has primarily to do with the degree of specialization of the “owning” user community and the globalization benefits derived by the importing. Generic vulnerability and incident specifications, for example, have broad applicability; while evidence information exchange specifications may not.

These structured information capabilities are organized into several exchange “clusters” for distinct cybersecurity user groups and requirements. The clusters are broad classifications and elements in one cluster may actually be used in one or more other clusters, depending on the application. Identified needs include:

- Weakness, vulnerability and state exchange
- Event, incident, and heuristics exchange
- Evidence exchange
- CIRT Policy exchange
- Cybersecurity organization identity and assurance
- Cybersecurity heuristics and information request

Those dependencies – as explained in the CYBEX ontology above – result in an effective cybersecurity ecosystem where knowledge derived from reports, testing, experience, and experience are used to create and evolve the weakness and vulnerability information that in turn can be used together with system state information to “measure” and enhance security. These building blocks can also be used for creating extension capabilities that include detection of malware or automating known secure “states” of software, services, and systems. This cybersecurity ecosystem enabled by CYBEX is shown in Figure 5, below. Evidence is produce when required by authorities for wrongdoing.

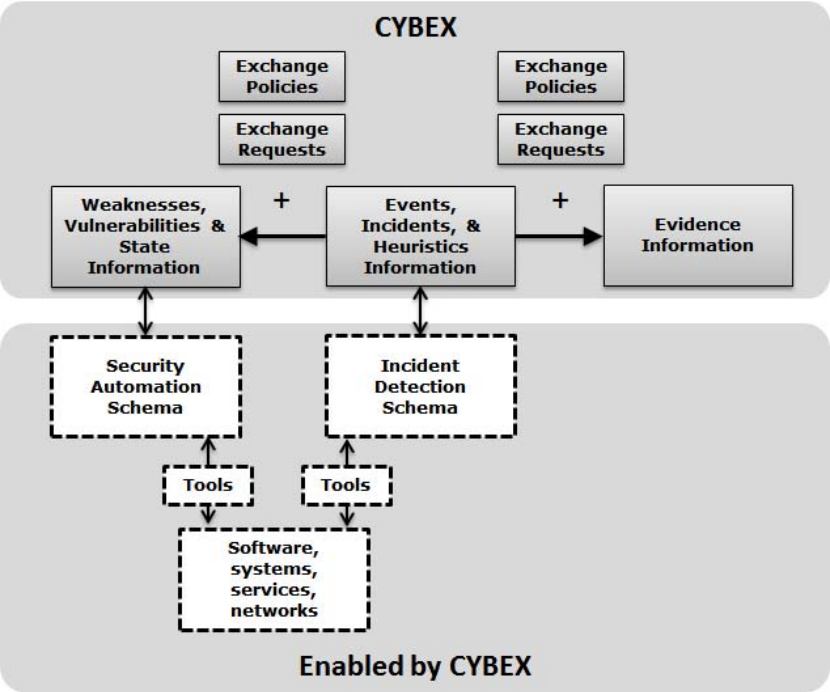

Figure 5 – The cybersecurity ecosystem enabled by CYBEX

7.1 Weakness, Vulnerability and State Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging weakness and vulnerability information and/or assessing the state of systems, applications, etc. The cluster includes extensions of these specifications that are specific to applications such as SmartGrid and eHealth IT cybersecurity. The specification order is based on dependencies depicted in Fig. 6, below.

Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures is an XML based specification for exchanging information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." CVE is designed to allow vulnerability databases and other capabilities to be linked together, and to facilitate the comparison of security tools and services. As such, CVE does not contain information such as risk, impact, fix information, or detailed technical information. CVE only contains the standard identifier number with status indicator, a brief description, and references to related vulnerability reports and advisories. The intention of CVE is to be comprehensive with respect to all publicly known vulnerabilities and exposures. While CVE is designed to contain mature information, the primary focus is on identifying vulnerabilities and exposures that are detected by security tools and any new problems that become public, and then addressing any older security problems that require validation. Ref X.cve

Common Vulnerability Scoring System (CVSS). The Common Vulnerability Scoring System specification provides for an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to

any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting a common language of scoring IT vulnerabilities. Ref X.cvss

Common Weakness Enumeration (CWE). Common Weakness Enumeration is an XML/XSD based specification for exchanging unified, measurable sets of software weaknesses that enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design. CWE implementations are compiled and updated by a diverse, international group of experts from business, academic institutions and government agencies, ensuring breadth and depth of content. CWE provides standardized terminology, allows service providers to inform users of specific potential weaknesses and proposed resolutions, and allows software buyers to compare similar products offered by multiple vendors.

Common Weakness Scoring System (CWSS). The Common Weakness Scoring System specification provides for an open framework for communicating the characteristics and impacts of software weakness.

Open Vulnerability and Assessment Language (OVAL). Open Vulnerability and Assessment Language is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

Three OVAL schemas written in Extensible Markup Language (XML) have been developed to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

eXensible Configuration Checklist Description Format (XCCDF). The eXtensible Configuration Checklist Description Format is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. XCCDF documents are expressed in XML.

Common Platform Enumeration (CPE). Common Platform Enumeration is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Common Configuration Enumeration (CCE). Common Configuration Enumeration provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of

configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.

Assessment Result Format (ARF). Assessment Results Format (ARF) is an open specification that provides a structured language for exchanging per-device assessment results data between assessment tools, asset databases, and other products that manage asset information. It is intended to be used by tools that collect detailed configuration data about IT assets. ARF is the per-device results language specification in CYBEX that enables the reporting of assessments of IT assets in an enterprise environment, known collectively as security automation interfaces. The ARF Policy Language for Assessment Results Reporting (PLARR) specification is the request specification while ARF's Assessment Summary Results (ASR) is the multi-device assessment results format in the suite. The security automation interfaces specifications describe an end-to-end process for delivering assessment content to data stores, requesting assessments against that content, reporting on the results of those assessments, and aggregating assessment results to an enterprise level.

7.2 Event, Incident, Heuristics Exchange Cluster

The following specifications are included as part of the framework for the purpose of exchanging observed event, incident or heuristic information in a structured fashion among Information Security Response Teams and others to create a comprehensive means of both responding to attacks as well as reduce weaknesses and vulnerabilities in systems as described in the CYBEX ontology in Sec. 6, above.

Common Event Expression (CEE). Common Event Expression standardizes the way computer events are described, logged, and exchanged. By using CEE's common language and syntax, enterprise-wide log management, correlation, aggregation, auditing, and incident handling can be performed more efficiently and produce better results. The primary goal of the effort is to standardize the representation and exchange of logs from electronic systems. CEE breaks the recording and exchanging of logs into four (4) components: the event taxonomy, log syntax, log transport, and logging recommendations.

Rec. ITU-T X.iodef, Incident Object Description Exchange Format (IODEF). The Incident Object Description Exchange Format defines a data representation that provides a framework for the exchange of information commonly exchanged by Computer Security Incident Response Teams (CIRTs) about computer security incidents. This document describes the information model for the IODEF and provides an associated data model specified with XML Schema.

Common Attack Pattern Enumeration and Classification (CAPEC). CAPEC is an XML/XSD based specification for the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of CAPEC is to provide a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy.

Phishing, Fraud, and Misuse Format. The Phishing, Fraud, and Misuse Exchange Format extends the Incident Object Description Exchange Format (IODEF) to support the reporting of phishing, fraud, other types of electronic crime. The extensions also support the exchange on information about widespread spam incidents. These extensions are flexible enough to support information gleaned from activities throughout the entire electronic fraud or spam cycle. Both simple reporting and complete forensic reporting are possible, as is consolidating multiple incidents.

"Misuse" in this context refers to the unlawful use of certificates and marks in the course of an on-line transaction – usually to perpetuate a fraud.

Malware Attribution Enumeration and Characterization Format. The Malware Attribution Enumeration and Characterization Format (MAEC) is a formal language for characterizing malware with two core components consisting of enumerated elements (vocabulary) and schema (grammar). Multiple levels of abstraction focus on attributes and behaviors.

7.3 CIRT Policy Exchange Cluster

[ed. Ref. Traffic Light Protocol (RLP), EC National and European Information Sharing and Alerting System (NEISAS) project, related ENISA projects, and IODEF features to support CIRT policy exchange capabilities.]

7.4 Evidence Exchange Cluster

The following specifications are included as part of the framework for the purpose of acquiring and handing over evidence to law enforcement authority or juridical bodies when required by those authorities or bodies.

Handover Interface and Service-Specific Details (SSD) for IP delivery. The Handover Interface and Service-Specific Details (SSD) for IP delivery specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a law enforcement facility to provide an array of different real time network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules. [ETSI TS102232]

Handover Interface for the Request and Delivery of Retained Data. The Handover Interface for the Request and Delivery of Retained Data specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a law enforcement facility to provide an array of different stored network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules and XML schema. [ETSI TS102657]

Architecture for Lawful Intercept in IP Networks. The Architecture for Lawful Intercept in IP Networks specification defines a data representation that provides a framework for the exchange of information between a network access point and a provider mediation facility to provide an array of different real time network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with ASN.1 modules. [IETF RFC3924]

Handover for Location Services. The Handover Interface for Location Services specification defines a data representation that provides a framework for the exchange of information between a network mediation point and an external facility to provide a real-time or stored location forensics associated with a network device. This document describes the information model and provides an associated data model specified with ASN.1 modules and XML schema. [3GPP TS23.271]

Electronic Discovery Reference Model. The Electronic Discovery Reference Model specification defines a data representation that provides a framework for the exchange of information between a network mediation point and a juridical designated party to request and provide an array of different stored network forensics associated with a designated incident or event. This document describes the information model and provides an associated data model specified with XML schema. [ERDM]

Digital Evidence Exchange Format. The Digital Evidence Exchange Format specification defines structures and data elements for structured digital evidence exchange file exchange. Electronic evidence means information and data of investigative value that is stored on or transmitted by electronic device. The primary purpose of digital evidence exchange format is interoperability of digital forensic systems. It does not include any protection scheme.

7.5 Cybersecurity Heuristics and Information Request Cluster

The following specifications are included as part of the framework for the purpose of requesting cybersecurity heuristics and information.

Cybersecurity Heuristics and Information Request Protocol. (CYIQL) Cybersecurity Heuristics and Information Request Protocol defines a flexible data representation that provides a framework for requesting information commonly exchanged by Computer Security Incident Response Teams (CIRTs) about computer security incidents. This document describes the information model for CHIRP and provides an associated data model specified with XML Schema.

7.6 Relationships and dependencies among cybersecurity structured information specifications and derivative extensions

The structured information specifications have relationships with the CYBEX ontology shown in Figure 6, below.

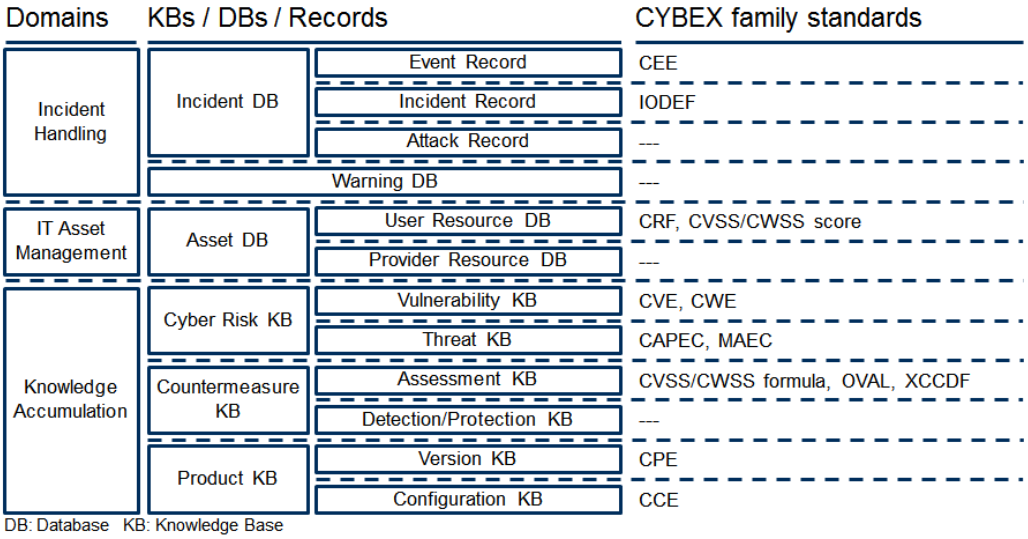

Figure 6 - Cybersecurity structured information specification relationships with the CYBEX ontology

These specifications also have multiple dependencies among themselves as well as with many possible applications. See Figure 7. The special case of malware information exchange using MAEC is in Figure 8, below.

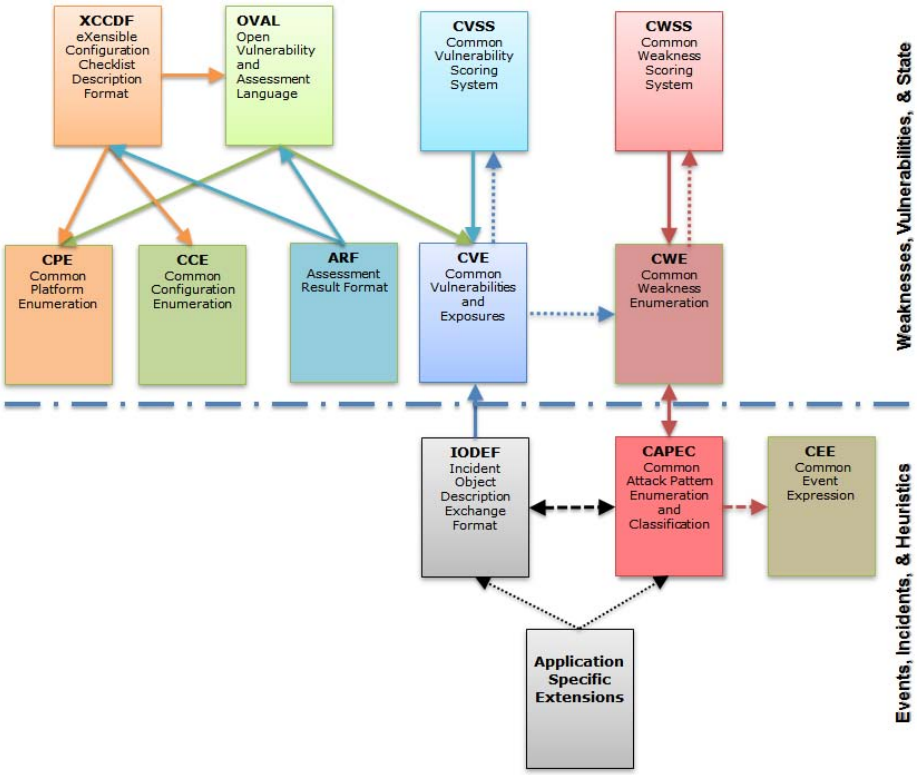

Figure 7 – Relationships and dependencies among structured information exchange capabilities

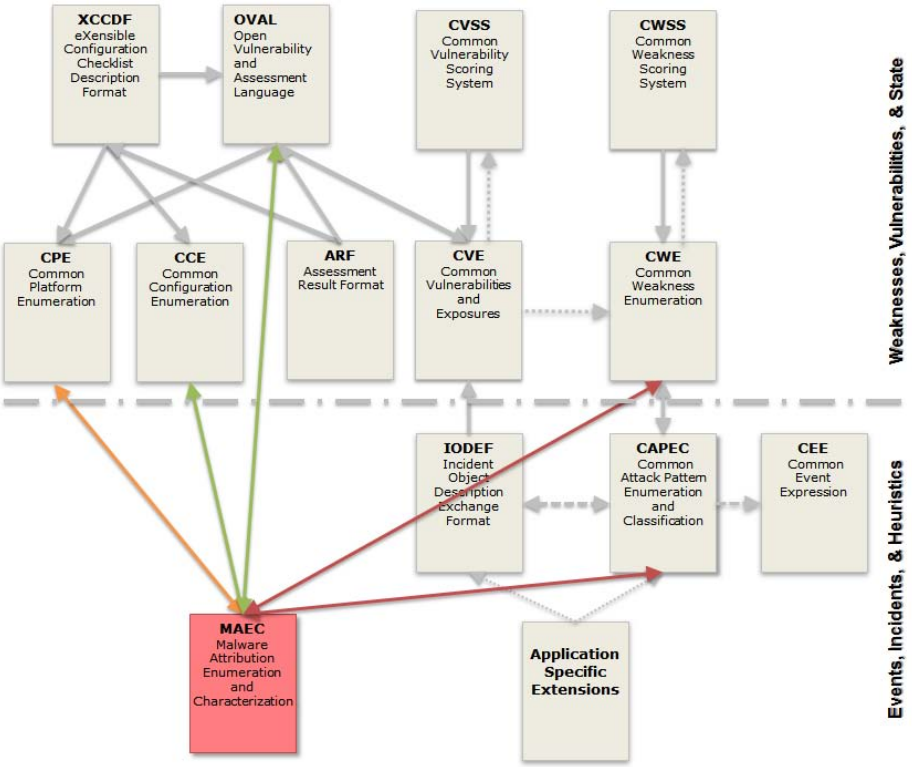

Figure 8 – Malware behaviour observation description capabilities

7.7 Cybersecurity entity identification and discovery

Different cybersecurity organizations are implementing common cybersecurity protocols for the capture and exchange of system state, vulnerability, incident forensics, and incident heuristics information in operational applications and as specified in this Recommendation. As this information is becoming available from many different sources, implementers should harmonize how they identify cybersecurity organizations, trust and information exchange policies, and the information itself that is exchanged or distributed.

Any globally unique identifier used for global cybersecurity information exchange must necessarily have the following characteristics:

- simplicity, usability, flexibility, extensibility, scalability, and deployability;
- distributed management of diverse identifier schemes;
- long-term reliability of identifier registrars, and the availability of high-performance tools for discovering information associated with any given identifier

Discovery Mechanisms in the Exchange of Cybersecurity Information. This recommendation provides methods and mechanisms which can be used to identify and locate sources of cybersecurity information, types of cybersecurity information, specific instances of cybersecurity information, methods available for access of cybersecurity information as well as policies which may apply to the access of cybersecurity information.

7.8 Common Cybersecurity Identifier (CCI)

Cybersecurity information exchange protocols can be used by anyone, anywhere, at any time. So there is no way to control their use. However, common interests may exist among cybersecurity communities regarding cybersecurity identifiers and their creation, administration, discovery, verification, and use. Some of those interests include:

- Enhance the value of the cybersecurity information by enabling widespread exchange of the related event information and analysis of events over long periods of time
- Enhance the security of cybersecurity information exchanges by enabling identifier information to be obtained for verification and the related policies to be known
- Enhance the flexibility of cybersecurity of cybersecurity information exchanges by enabling new or additional information associated with the message to be obtained, e.g., information status

Guidelines for Administering the OID arc for cybersecurity information exchange. A common global cybersecurity identifier namespace for these purposes is described in Rec. ITU-T X.cybex.1, together with administrative requirements, as part of a coherent OID arc, and includes:

- Cybersecurity information identifiers
- Cybersecurity organization identifiers
- Cybersecurity policy identifiers

8. Cybersecurity assured exchange

Within the Information Exchange Framework, the actual exchange of structured information can occur many different ways – via a network or physically transported. A key element for this exchange is trust – trust in the identity of the parties as well as the information being conveyed. The latter can have additional requirements imposed if the exchanged information is subsequently used for evidentiary purposes.

8.1 Assurance of Identities

Many different trust assurance mechanisms are used in conjunction with the exchange of cybersecurity information. Several are included as part of this framework.

Entity authentication assurance. This Recommendation | International Standard provides an authentication life cycle framework for managing the assurance of an entity's identity and its associated identity information in a given context. Specifically it provides methods to 1) qualitatively measure and assign relative assurance levels to the authentication of an entity's identities and its associated identity information, and 2) communicate relative authentication assurance levels.

Extended Validation Certificate Framework. The Extended Validation Certificate Framework consists of an integrated combination of technologies, protocols, identity proofing, lifecycle management, and auditing practices that describe the minimum requirements that must be met in order to issue and maintain Extended Validation Certificates ("EV Certificates") concerning a subject organization. The framework accommodates a wide range of security, localization and notification requirements.

ETSI TS102042 V.2.1, Policy requirements for certification authorities issuing public key certificates. The present document specifies policy requirements relating to Certification Authorities (CAs) issuing public key certificates, including Extended Validation Certificates (EVC). It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.

8.2 Information Exchange Protocols

This section contains specific exchange protocols that are used in diverse cybersecurity information exchange contexts.

Transport Protocols supporting Cybersecurity Information Exchange. This recommendation provides an overview of exchange protocols which have been adopted and or adapted for use within the Cybersecurity Information Exchange Framework, Cybex.

Blocks eXtensible eXchange Protocol Framework for CYBEX. RFC3080 describes a generic application protocol kernel for connection-oriented, asynchronous interactions called BEEP. At BEEP's core is a framing mechanism that permits simultaneous and independent exchanges of messages between peers. Messages are arbitrary MIME content, but are usually textual (structured using XML). All exchanges occur in the context of a channel -- a binding to a well-defined aspect of the application, such as transport security, user authentication, or data exchange. Each channel has an associated "profile" that defines the syntax and semantics of the messages exchanged. Implicit in the operation of BEEP is the notion of channel management. In addition to defining BEEP's channel management profile, this document defines: the TLS transport security profile; and,

the SASL family of profiles. Other profiles, such as those used for data exchange, are defined by an application protocol designer.

Simple Object Access Protocol for CYBEX. SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.

Transport of Real-time Inter-network Defense (RID) Messages. This specification specifies the transport of RID messages within HTTP [RFC2616] Request and Response messages transported over TLS.

ETSI TS102232-1, Handover Interface and Service-Specific Details (SSD) for IP delivery. The -1 module of the Handover Interface and Service-Specific Details (SSD) for IP delivery specification contains protocols and their implementation for trusted delivery of forensic information to law enforcement and security authorities.

Appendix A – Security Automation Schema Use Cases

Introduction. [TBD]

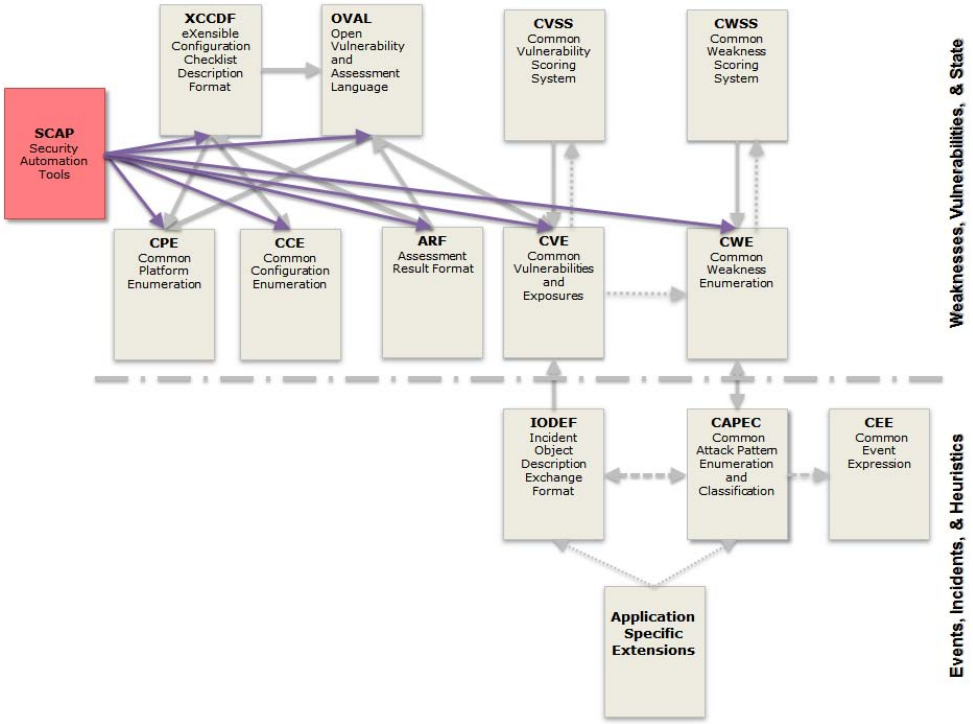

Figure 8 – Cybersecurity Assurance and Integrity Automation

NIST Security Content Automation Protocol (SCAP). The NIST Security Content Automation Protocol is one of the most developed and best known Security Automation Schema. It comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. This technical specification describes the requirements and conventions that are to be employed to ensure the consistent and accurate exchange of SCAP content and the ability of the content to reliably operate on SCAP validated tools. The initial version is comprised of the six specifications: XCCDF, OVAL, CPE, CCE, CVE, and CVSS as depicted above in Figure 8. These specifications are grouped into three categories: languages, enumerations, and vulnerability measurement and scoring systems.

Appendix B: compendium of cybersecurity requirements and guidelines

This appendix contains an extensive compendium of existing requirements that provide the basis for the Cybersecurity Information Exchange Framework as well as guidelines for its use.

Generic Cybersecurity

X.1205	Overview of cybersecurity
X.gopw	Guideline on preventing malicious code spreading in a data communication network
WD27032	Guidelines for cybersecurity
WD27033-1	Guidelines for Network security
WD27034	Application security
Y.2701	Next Generation Network security
X.tsgf	Information security governance framework
WD27014	Information security governance framework
IS 27001	Information security management system requirements
IS 27002	Information security management Code of practice
IS 27010	Information security management for inter-sector and inter-organisational communication

Vulnerability Exchange

X.1206	automatic notification of security related information and dissemination of updates
IS 15408, 18045	Evaluation Criteria for IT security, International Common Criteria Project
IS 15292	Protection Profile registration procedures
IS 19791	Security Assessment of Operational Systems
WD29147	Vulnerability disclosure

Generic Security Information

X.sisfreq	Capabilities and their context scenarios for cybersecurity information sharing and exchange
X.gpn	Mechanism and procedure for distributing policies for network security

Incident Forensics

X.1056	Security Incident Management for telecommunications organizations
WD27035	Information Security Incident Management
X.bots	Framework for botnet detection and response
X.tb-ucc	Traceback use cases and capabilities
X.abnot	Abnormal traffic detection and control guideline for telecommunication network
X.sips	Framework for countering cyber attacks in SIP-based services
Y.dpireq	NGN deep packet inspection requirements
WD27037	Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Evidence

TS102656	Retained Data Requirements
TS101331	Requirements of Law Enforcement Agencies