INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

TD 1161

English only

Original: English

Question(s): 4/17 Geneva, 8-17 December 2010

TEMPORARY DOCUMENT

Source: Editors, CYBEX Correspondence Group

Title: Draft Recommendation ITU-T X.1500 [X.cybex], *Cybersecurity information exchange framework*

Contact:	Stephen Adegbite Adobe, FIRST USA	Tel: +1 415 832 4292 Email: sadegbit@adobe.com
Contact:	Inette Furey Department of Homeland Security USA	Tel: +1 703-235-5824 Email: Inette.Furey@dhs.gov
Contact:	Dr. Youki Kadobayashi NICT Japan	Tel: +81 74 372 5210 Email: youki-k@is.naist.jp
Contact:	Robert A. Martin MITRE USA	Tel: +1 781 271 3001 Email: ramartin@mitre.org
Contact:	Damir Rajnovic FIRST UK	Tel: +44 7715 546 033 Email: drajnovi@cisco.com
Contact:	Gavin Reid Cisco USA	Tel: +1 408 894 8887 Email: gavreid@cisco.com
Contact:	Tony Rutkowski Yaana Technologies USA	Tel: +1 408 854 8041 Email: tony@yaanatech.com
Contact:	Gregg Schudel Cisco USA	Tel: +1 571 332 2222 Email: gschudel@cisco.com
Contact:	Dr. Takeshi Takahashi NICT Japan	Tel: +81 42 327 5862 Email: takeshi_takahashi@nict.go.jp

Introduction

The annex to this document contains proposed draft Recommendation ITU-T X.1500, *Cybersecurity information exchange framework*, for determination at the SG17 December 2010 meeting. This proposed action and the work were re-approved by SG17 at the April 2010, Geneva, meeting (TD 0943 Rev.2).

The editors initially designated for the progress of the Recommendation were (in alphabetical order): Stephen Adegbite (Adobe, FIRST), Inette Furey (DHS), Youki Kadobayashi (NICT), Robert A. Martin (MITRE), Angela McKay (Microsoft), Damir Rajnovic (FIRST), Gavin Reid (Cisco), Tony Rutkowski (Yaana), Gregg Schudel (Cisco). As the work progressed, Takeshi Takahashi (NICT) was added, and Angela McKay was unable to continue.

The draft was reviewed and edited in detail at the Q.4/17 October Interim Meeting at Tokyo, and accepted with further changes indicated in the document for editing by the CYBEX Correspondence Group and submission to the December 2010 meeting for determination. See Q4-2010-Oct-Doc-002R3, and the report, Q4-2010-Oct-Doc-006R1.

This draft includes substantial continuing work since the CYBEX framework was initially conceived at February 2010 Study Group 17 meeting and evolved at multiple subsequent meetings (Q4/17, Geneva, June 2009; SG17, Geneva, Sept 2009; Q4, Redmond, Nov 2009; Q4, Sophia-Antipolis, Jan 2010; SG17, Geneva, Apr 2010; Q4, eMeeting, July 2010; and Q4, Tokyo, Oct 2010) and via frequent teleconferences. The work includes not only that of the editors and others present at these meetings and teleconferences, but also the multiple participating cybersecurity user communities associated with the specifications included in the Framework. As a result, it can be stated with some confidence that global cybersecurity will be significantly enhanced by the adoption of this Recommendation and its continuing evolution.

Appendix:

> Draft Recommendation ITU-T X.1500 [X.cybex], *Cybersecurity information exchange framework*

X.1500 [X.cybex]

Recommendation ITU-T X.1500 [X.cybex]
Cybersecurity information exchange framework

Summary

This Recommendation

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

b) enables this exchange by
- identifying and incorporating existing capability specifications 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.

This framework is adaptable, extensible, and non-prescriptive to allow the capability specifications – some of which are continuously evolving in varying stages of completion – to be applied in different instantiations to enhance cybersecurity of telecommunication/ICT infrastructure, devices, and services. This framework will be revised as those specifications evolve.

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 facilitated secure collaborative processes and controls, including those for Secure Online Transactions, which raise the level of assurance between organizations exchanging the information and thereby 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 facilitates the scaling and broad implementation of core assurance, operational risk management, and response capabilities – many of which have already been developed and are evolving 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 by describing 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
- enabling assured cybersecurity information exchange

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 the following exchange “clusters” :

- Weakness, vulnerability and state exchange
- Event, incident, and heuristics exchange
- Policy exchange
- Evidence exchange
- Identification and discovery
- Identity assurance
- Exchange

X.1500 [X.cybex]

Recommendation ITU-T X.1500 [X.cybex]
Cybersecurity Information Exchange Framework

Table of Contents

History

Sep 2009	Initial draft (including TSB Director-SG17 chair editorial change of CYBIEF to CYBEX)
Apr 2010	SG17 Meeting revision
Dec 2010	[SG17 Meeting revision and determination]

RECOMMENDATION ITU-T X.1500 [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
- enabling assured cybersecurity information exchange

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 E.409] ITU-T Recommendation X.1205 (2004-05), *Incident organization and security incident handling: Guidelines for telecommunication organizations*

[ITU-T X.1205] ITU-T Recommendation E.409 (2008-04), *Overview of cybersecurity*.

3. Definitions

3.1 Terms defined elsewhere

3.1.1 cybersecurity [X.1205]

3.2 Terms defined in this Recommendation

3.2.1 **capability instantiation (instance)**: refers to an implemented set of specifications.

3.2.2 **capability specification (specification)**: refers to a set of rules governing the structure, syntax and expectations for the presentation or exchange of data.

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

3.2.4 **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.

3.2.5 **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

3.2.6 **cybersecurity operations**: Methods and processes used to monitor and manage security within defined operational limits including:

- The collection and analysis of information which may have an effect on security.
- The detection of behavior or events which adversely affect security or by which the likelihood of a future adverse effect can be determined.
- Action taken as a result of adverse behavior or event taking place in order to limit, mitigate and/or prevent future incidents.
- Security-related communications concerning the status and condition of systems.

3.2.7 **exchange protocol**: A set of technical rules and associated behavior governing the exchange of information between two or more computer systems via a network.

3.2.8 **security incident:** Any adverse event whereby some aspect of security could be threatened [E.409]

3.2.9 **policy:** Terms and conditions associated with the use and sharing of cybersecurity information

3.2.10 **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	Asset Reporting 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
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
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
TLP	Traffic Light 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. 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.

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
- enabling assured cybersecurity information exchanges

Clauses 7 and 8 of this Recommendation describe means for accomplishing these functions.

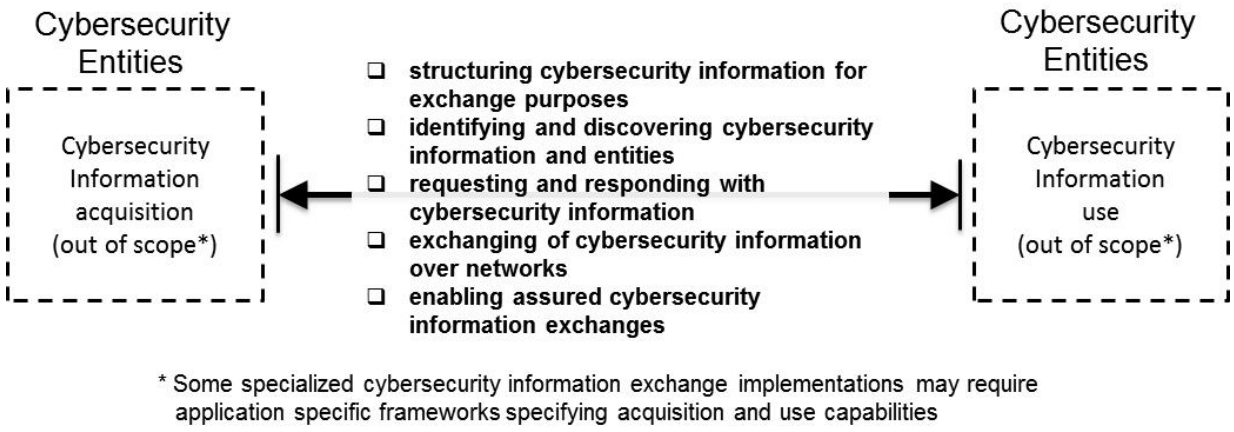

Figure 1 – Framework for the exchange of cybersecurity information

The exchange framework is bi-directional. This bi-directionality allows for verified information requests and 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 information exchange implementations such as traceback of attack sources may require application specific frameworks. Such implementations will provide acquisition and use capabilities applicable 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 and manageable, for example, through the use of security content automation capabilities.

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

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 exchanges among elements indicated by dashed lines 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. In Figure 2, CIRT activities typically encompass all the measures that enable threat detection and thwarting or other remedies.

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

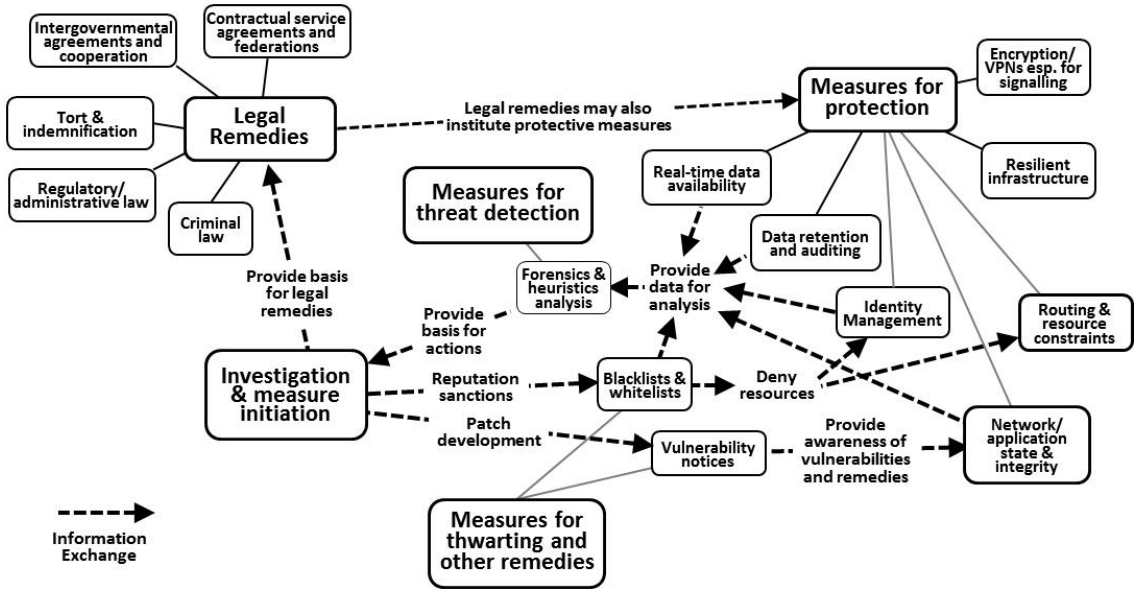

Figure 2 – Cybersecurity elements supported by cyber security information exchange

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 indicate the relationship of the information types, while arrows indicate information input from an entity to a knowledge base/database. The functions shown on the right are generic and entities such as CIRTs may encompass one or more of these functions.

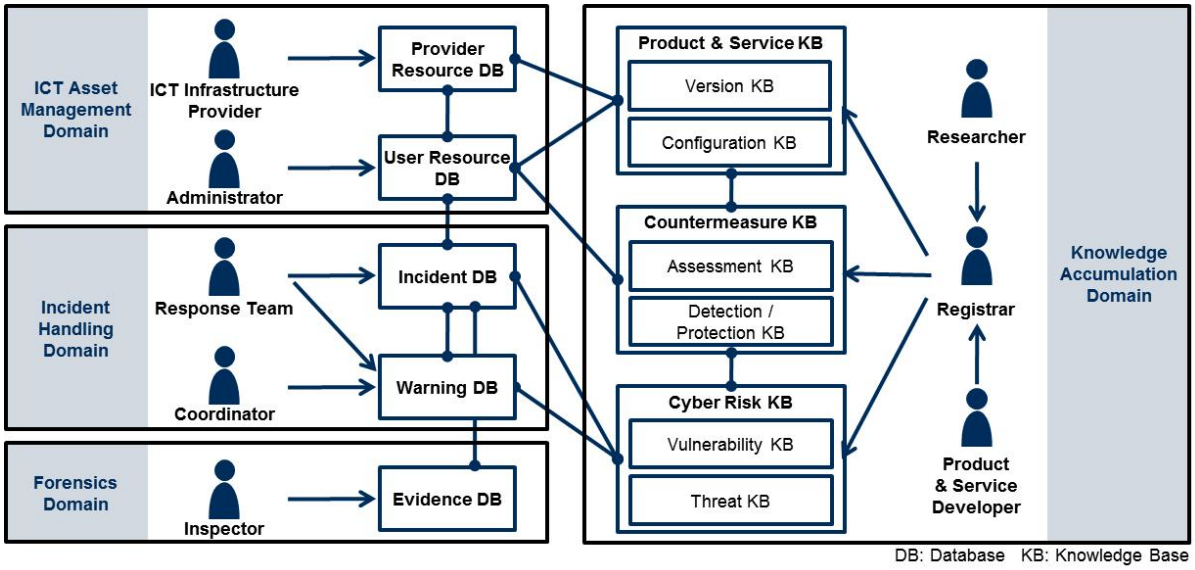

Figure 3 - CYBEX ontology model

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. In the following

subclauses, a detailed ontology is 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.

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

In the Knowledge Accumulation Domain, three operation entities exist: Researcher, Product & Service Developer and Registrar. A Researcher researches cybersecurity information, 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 Researchers, Developers, and Vendors so that the knowledge can be used for another organization.

6.3.3 Cybersecurity Operational Information

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

6.3.3.1 Incident Handling Domain

In the Incident Handling Domain, there exist an Incident Database and a Warning Database 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 privileged users logging into a system. It also includes information on packets, files and transactions related to incidents. 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 a Response Team and Coordinator. The warnings are based on the Incident Database as well as the Cyber Risk Knowledge Base.

6.3.3.2 ICT Asset Management Domain

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

The User Resource Database accumulates information on assets inside an 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 results, and intranet topology. The information is provided by the Administrator.

The Provider Resource Database accumulates information on assets outside the individual organization. It mainly contains external resource information and external network information. External resource information consists of 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 consists of information on networks that connect each organization to other organizations such, as their topology, routing information, access control policy, traffic status and the security level. The information is provided by the ICT Infrastructure Provider.

6.3.3.3 Knowledge Accumulation Domain

Three knowledge bases exist in the Knowledge Accumulation Domain: Cyber Risk, Countermeasure, and Product & Service. They accumulate knowledge on cybersecurity provided by the 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 vulnerabilies. It also includes human vulnerabilities exposed by human ICT users. The Threat Knowledge Base accumulates known threat information that includes attack knowledge and misuse knowledge. Attack knowledge includes 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 about past attacks. Misuse knowledge includes information about misuses of ICT 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 the security level of ICT 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.

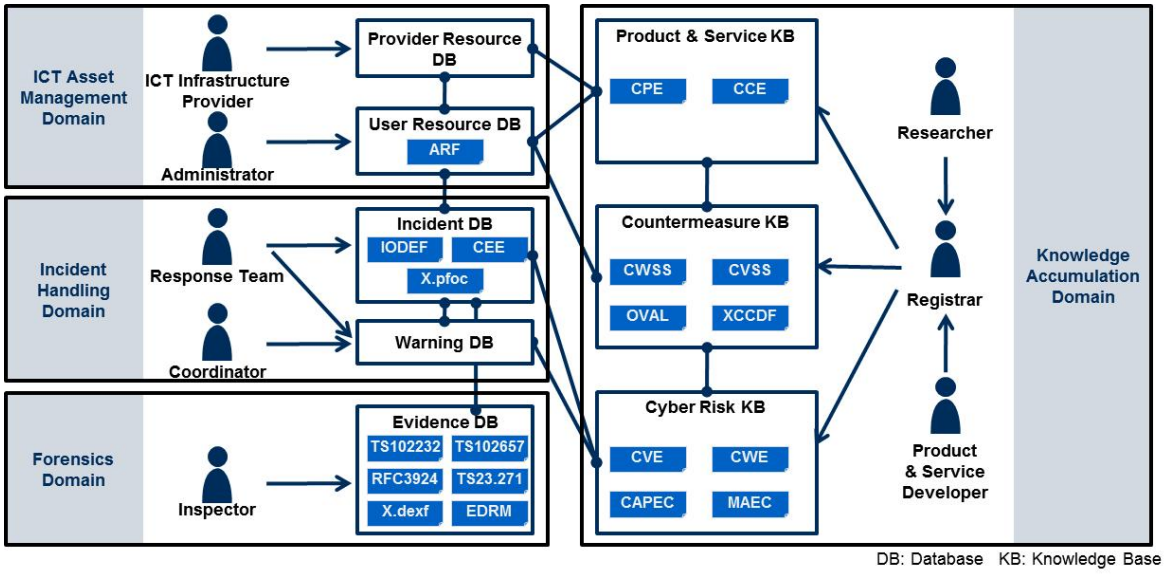

Figure 4 - Detailed view of the CYBEX ontology model

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

7. Structured cybersecurity 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 clause describes specifications that enable this exchange. The goal is to make it easier to share cybersecurity information that 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 facilitates cybersecurity related comparisons. Subsequent clauses of this Recommendation treat other essential parts of the framework such as cybersecurity identification, discovery, and assured exchange.

Some existing specifications are being imported as X-series Recommendations while others are simply identified. 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 some 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 capabilities in one cluster may actually be used in one or more other clusters, depending on the application. Identified clusters of capabilities include:

- Weakness, vulnerability and state exchange
- Event, incident, and heuristics exchange
- Policy exchange
- Evidence exchange
- Identification and discovery
- Identity assurance
- Exchange

These capabilities – as put in an operational context by the CYBEX ontology above – result in an effective cybersecurity ecosystem where knowledge derived from reports, testing, 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 relationships between the ontology and capabilities are explained in further detail in subclause 7.6.

These capabilities can also be used for creating specific CYBEX instantiations that include automating known secure or trusted “states” of software, services, and systems, detecting malware, capturing incident and heuristics information; and if necessary, producing evidence for enforcement purposes. This integration enabled by CYBEX is shown in Figure 5 below, and Appendix A contains examples of such instantiations.

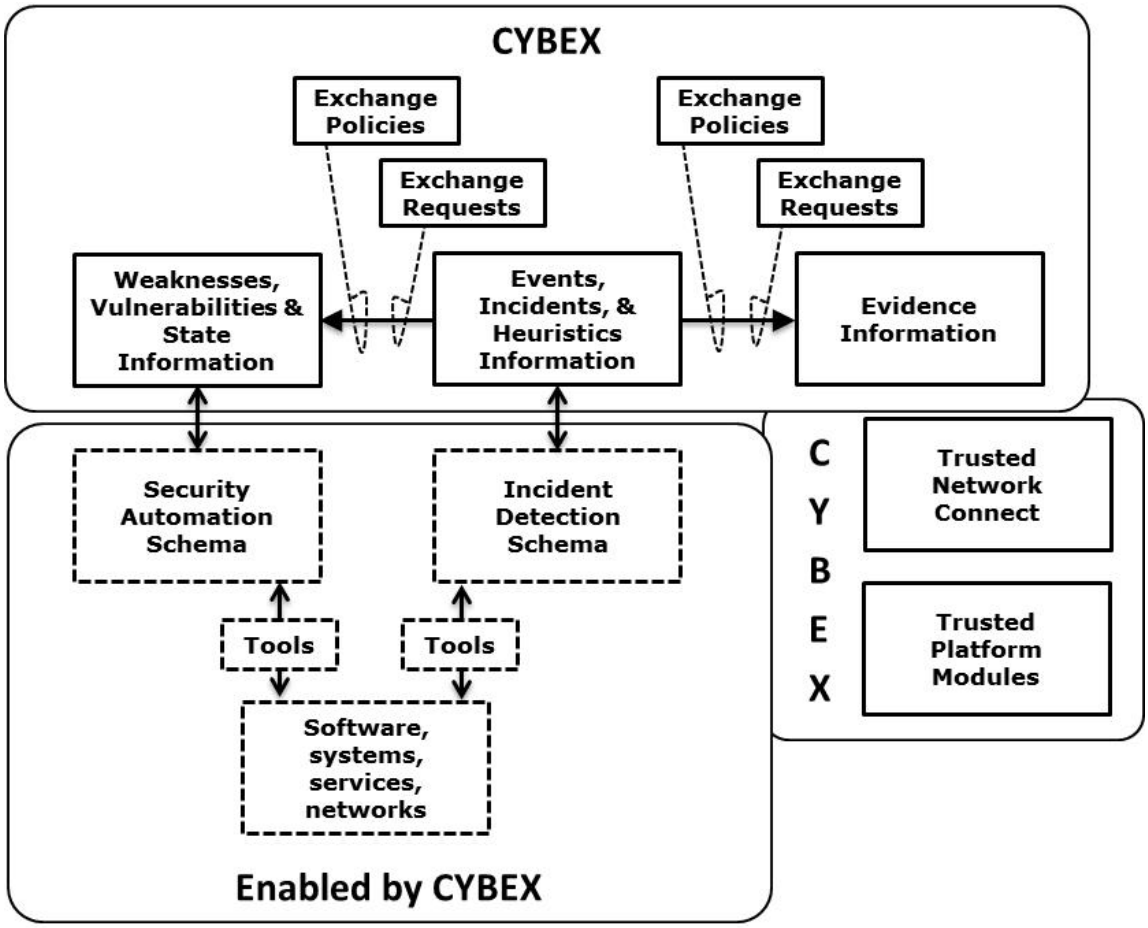

Figure 5 – Cybersecurity instantiations enabled by CYBEX

In this depiction, CYBEX clusters are shown as an ensemble of cybersecurity instantiations together with associated systems and tools that make use of the structured information exchange capabilities. The CYBEX framework in this Recommendation identifies an array of interoperable protocols and other specifications that enable and significantly facilitate these instantiations. The dashed depictions are capabilities not specified in the CYBEX framework, but rely on the framework for their implementation. The CYBEX Trusted Platform Modules and Trusted Network Connect capabilities are depicted as underlying all other capabilities as enablers of enhanced assurance capabilities for cybersecurity information exchange and are entwined with the use of some exchange platforms such as OVAL that together enhance ICT security content attestations.

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. This cluster includes extensions of these specifications that are specific to applications such as SmartGrid and eHealth ICT cybersecurity. The specification order is based on dependencies depicted in Figures 6-8 below.

Common Vulnerabilities and Exposures (CVE). Common Vulnerabilities and Exposures is a specification for identifying and exchanging information security vulnerabilities and exposures, and that aims to provide common identifiers 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. Rec. ITU-T X.1520]

Common Vulnerability Scoring System (CVSS). The Common Vulnerability Scoring System specification provides for an open framework for communicating the characteristics and impacts of ICT 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 ICT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting a common language of scoring ICT vulnerabilities. [Ref Rec. ITU-T X.1521]

Common Weakness Enumeration (CWE). Common Weakness Enumeration is a specification for identifying and exchanging unified, measurable sets of software weaknesses. CWE enables more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems. It also provides for 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, academia 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 specification 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.

OVAL schemas written in 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 (CPE) is a standardized method to identify and describe the software systems and hardware devices present in an enterprise's computing asset inventory. CPE provides: a naming specification, including the logical structure of well-formed CPE names and the procedures for binding and unbinding these names with machine-readable encodings; a matching specification, which defines procedures for comparing CPE names to determine whether they refer to some or all of the same products or platforms; and a dictionary specification, which defines the concept of a dictionary of identifiers and prescribes high-level rules for dictionary curators.

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.

Asset Reporting Format (ARF). Asset Reporting 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. Along with ARF, there is an aggregate reporting specification to enable reporting on information across multiple assets and a tasking and query language to enable requesting assessment results. To enable identification of assets and correlation of asset data, there is also a specification for standardized identification of assets regardless of assessment or tool type. 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, and 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 Computer Incident Response Teams (CIRTS) 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 clause 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.

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 CIRTs about computer security incidents. IODEF describes an information model and provides an associated data model specified with XML Schema.

Common Attack Pattern Enumeration and Classification (CAPEC). CAPEC is a 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 XML 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. [Ref. IETF RFC 5901]

Malware Attribution Enumeration and Characterization Format. The Malware Attribution Enumeration and Characterization Format (MAEC) is a formal language that includes a schema to provide both a syntax for the common vocabulary of enumerated attributes and behaviors, and an interchange format for structured information about these data elements. The enumerations are at different levels of abstraction: low-level actions, mid-level behaviors and high-level mechanisms. At the lowest level, MAEC describes attributes tied to the basic functionality and low-level operation of malware. At the middle level, MAEC's language organizes the aforementioned low-level actions into groups for the purpose of defining mid-level behaviors. At the more conceptual and high level, MAEC's vocabulary allows for the construction of mechanisms that abstract clusters of mid-level malware behaviors based upon the achievement of a higher order classification.

7.3 Policy Exchange Cluster

The sharing and use of cybersecurity information between parties is usually accompanied by some kind of understanding concerning the terms and conditions associated with the information being shared. This understanding may be bound to the specific information being shared, or to the broad class of information to which it belongs, or be associated with the parties involved. To the extent it is necessary under the circumstances, it is desirable to provide notice of these policies to the parties involved. This notice may take many forms, and be conveyed together with the information or independently provided through a query-response mechanism. The protocols and requirements for policy exchange continue to emerge within information security exchange forums, and care should be taken to ensure their proper implementation.

Traffic Light Protocol (TLP). The Traffic Light Protocol (TLP) was created to encourage greater sharing of sensitive information. The originator signals how widely they want their information to be circulated beyond the immediate recipient. The TLP provides a simple method to achieve this. It is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way. The TLP is based on the concept of the originator

labeling information with one of four colors to indicate what further dissemination, if any, the recipient can undertake. The recipient must consult the originator if wider dissemination is required. The TLP is accepted as a model for trusted information exchange among security communities in over 30 countries. The four "information sharing levels" for the handling of sensitive information are:

> RED – Personal. This information is for named recipients only. In the context of a meeting, for example, RED information is limited to those present. In most circumstances RED information will be passed verbally or in person.
>
> AMBER - Limited distribution. The recipient may share AMBER information with others within their organization, but only on a "need-to-know" basis.
>
> GREEN - Community wide. Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community.
>
> WHITE - Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

[Information Sharing Levels, CPNI Information Exchange, UK CPNI (April 2010)]

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 authorities 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 Interface 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 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.

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

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

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

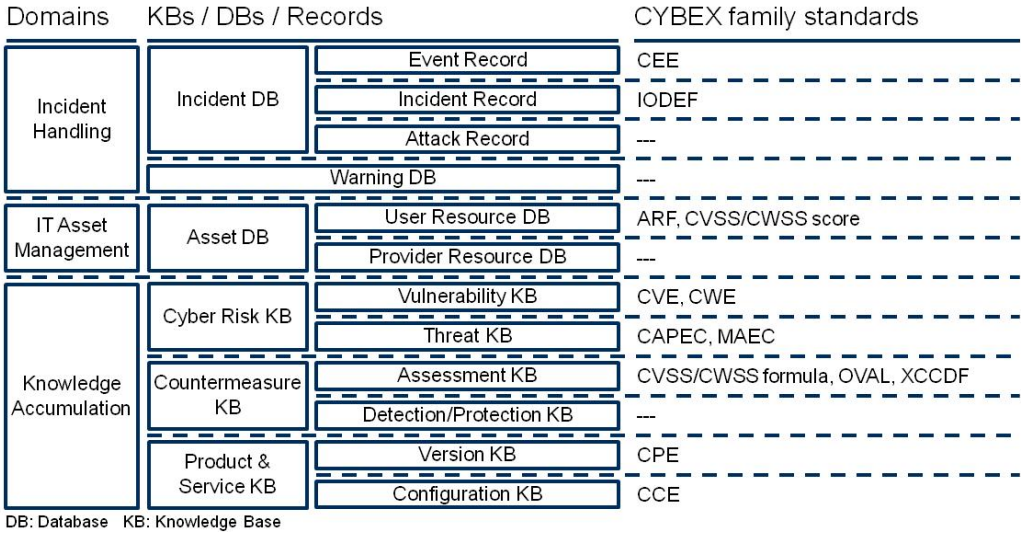

Figure 6 - Cybersecurity structured information specification relationships with the CYBEX ontology

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

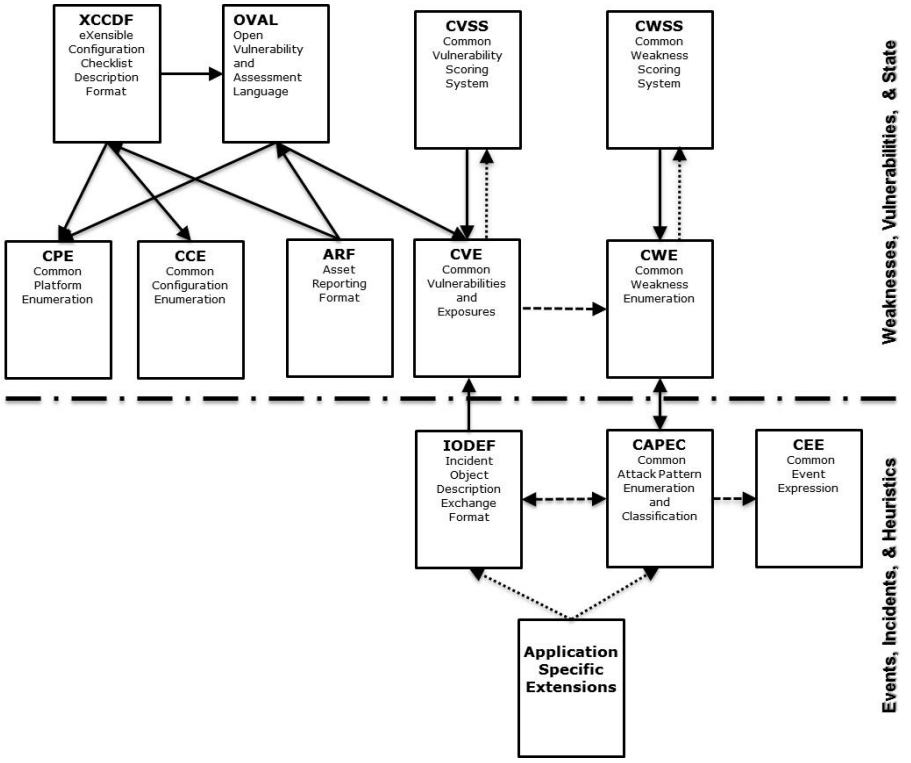

Figure 7 – Relationships and dependencies among structured information exchange capabilities

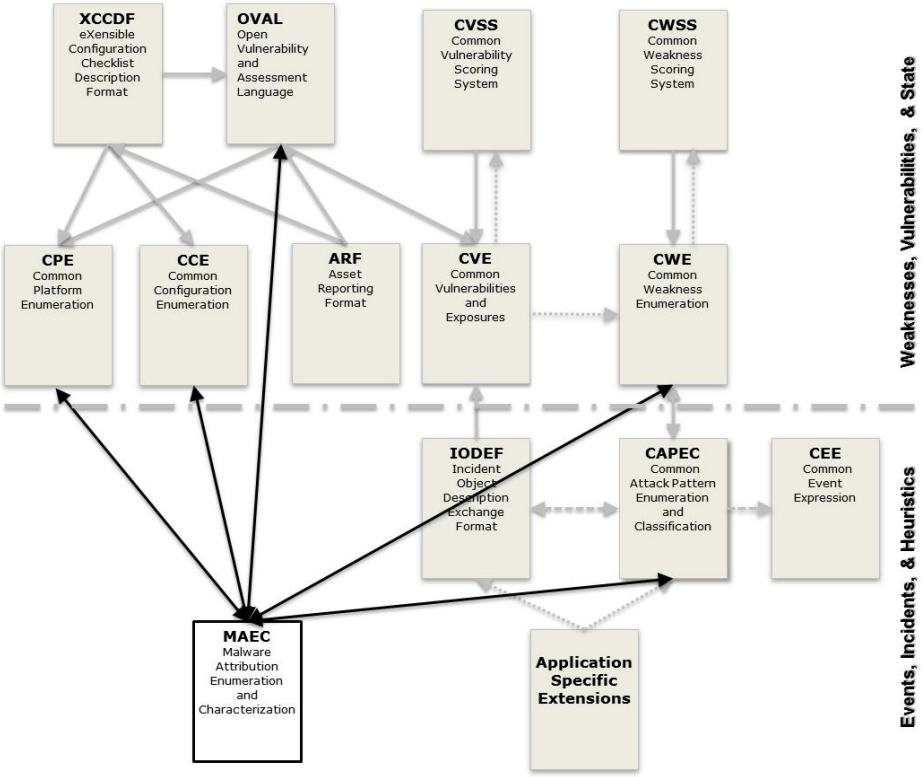

Figure 8 – Malware behavior observation description capabilities

8. Enabling cybersecurity information exchange

8.1 Identification, Discovery, and Queries Cluster

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 information exchanges by enabling new or additional information associated with the message to be obtained, e.g., information status

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.

Guidelines for Administering the OID arc for cybersecurity information exchange. A common global cybersecurity identifier namespace is described in Rec. ITU-T X.1500.1, together with administrative requirements, as part of a coherent OID arc, and includes identifiers for:

- Cybersecurity information
- Cybersecurity organization
- Cybersecurity policy

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

8.2 Identity Assurance Cluster

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.

Trusted platforms. Computing and communications products with embedded Trusted Platform Modules (TPMs) advance the ability of businesses, institutions, government agencies, and consumers to conduct trustworthy information exchange; therefore, TPMs are relevant to most CYBEX implementations. TPMs are special-purpose integrated circuits (ICs) built into a variety of platforms to enable strong user authentication and machine attestation - essential to prevent inappropriate access to confidential and sensitive information and to protect against compromised networks.

Trusted Platform Modules utilize open standards and technologies to ensure interoperability of diverse products in mixed-vendor environments. The prevalent TPM standard consists of a set of three specifications developed and maintained by the Trusted Computing Group (TCG), and have been adopted by the Common Criteria Control Board (CCDB) and re-published by ISO with the addition of an overview.

Specification Title	TCG Version (authoritative)	ISO/IEC Version
Overview		11889-1, 2009-05-15, Information technology — TPM — Part 1
Design Principles	TPM Main, Part 1, Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007	11889-2, 2009-05-15, Information technology — TPM — Part 2
TPM Structures	TPM Main, Part 2. Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007	11889-3, 2009-05-15, Information technology — TPM — Part 3
Commands	TPM Main, Part 3, Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007	11889-4, 2009-05-15, Information technology — TPM — Part 4

The design principles give the basic concepts of the TPM and generic information relative to TPM functionality. A TPM designer must review and implement the information in the TPM Main specification (parts 1-3) and review the platform specific document for the intended platform. The platform specific document contains normative statements that affect the design and implementation of a TPM. A TPM designer must review and implement the requirements, including testing and evaluation, as set by the TCG Conformance Workgroup. The TPM must comply with the requirements and pass any evaluations set by the Conformance Workgroup. The TPM may undergo more stringent testing and evaluation.

Trusted Network Connect. One goal of CYBEX is to discover the state of Operating System (OS)-level and application software by the supporting network. For example, when systems lack OS security patches or antivirus signatures, reliable notification is crucial to containing the damage associated with network- based attacks. Making this appraisal requires reliable information that a connected system is in a particular state.

In order to prevent systems from falsifying information - potentially due to adversary action - successful appraisal requires a hardware basis on the system to be appraised. As described in subclause 8.1, above, Trusted Platforms are embedded in the hardware to record certain facts about the boot process and deliver them in digitally signed form. Furthermore, major chip manufacturers are now supplementing the Trusted Platforms with a “late launch” capability that allows for

execution of trusted code later in the boot sequence. This, in turn, allows evidence to be reliably recorded after the hardware-specific boot process.

Network configuration management is effectively a deployment of system attestation: software agents on enterprise machines that periodically send configuration reports to a central repository, which evaluates and flags non-compliant systems. Data from these software agents, while valuable, is easily modified by an attacker. Using the widespread deployment of Trusted Platforms to enable a more trustworthy evaluation of system state would greatly increase an enterprise's confidence in its configuration management data.

This CYBEX goal is facilitated by Trusted Network Connect (TNC), which is an open architecture for network access control. Its aim is to enable network operators to provide endpoint integrity at every network connection, thus enabling interoperability among multi-vendor network endpoints. TNC currently consists of an extensive suite of standards all presently developed by the Trusted Computing Group, as shown in the table below.

Specification Title	TCG Version
Integrity Measurement Collectors	IF-IMC, Specification ver. 1.2 Rev. 8, 5 Feb 2007
Integrity Measurement Verifiers	IF-IMV Specification ver. 1.2 Rev. 8, 5 Feb 2007
Trusted Network Connect Client-Server	IF-TNCCS TLV Binding Specification ver. 2.0 Rev. 16, 22 Jan 2010
Trusted Network Connect Client-Server Statement of Health	IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan 2008
Policy Enforcement Point	IF-PEP Protocol Bindings for RADIUS Specification ver. 1.1 Rev. 0.7, 5 Feb 2007
Binding for SOAP	IF-MAP Specification ver. 2.0 Rev. 36, 30 Jul 2010
Platform Trust Services Interface	IF-PTS Specification ver. 1.0 Rev. 1.0, 17 Nov 2006
Clientless Endpoint Support Profile	CESP Specification ver. 1.0 Rev. 13, 18 May 2009

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. [CA/Browser Forum, Guidelines for the Issuance and Management of Extended Validation Certificates, Ver. 1.3]

Policy requirements for certification authorities issuing public key certificates. The specified 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. [ETSI TS102042]

8.3 Exchange Cluster

This sub-clause contains specific exchange protocols that are used in diverse cybersecurity information exchange contexts. It includes exchange protocols that have been adopted and/or adapted for use within the Cybersecurity Information Exchange Framework, CYBEX.

Blocks eXtensible eXchange Protocol (BEEP) 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 (SOAP) 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.

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. [**ETSI TS102232-1]**

Appendix A – Security Automation Schema Use Cases

As described in the introduction to clause 7, above, and depicted in Fig. 5, there are many possible implementations of the protocol clusters described in this CYBEX Framework Recommendation, with the object of achieving various levels of cybersecurity through the implementation of the capabilities depicted in Fig. 2, above.

It is expected that a very large number of implementations will emerge – particularly security automation schema for ensuring that ICT systems are properly configured and patched. Two initial prominent examples include: 1) the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) for implementing the United States Federal Desktop Core Configuration (FDCC) and its replacement, the United States Government Configuration Baseline (USGCB), and 2) the Japan JVN Security Content Automation Framework. In general, these security automation tool implementations take the form shown in Fig. 9, below, and include varied numbers of the CYBEX information exchange platforms represented by the overlay pointers in the diagram.

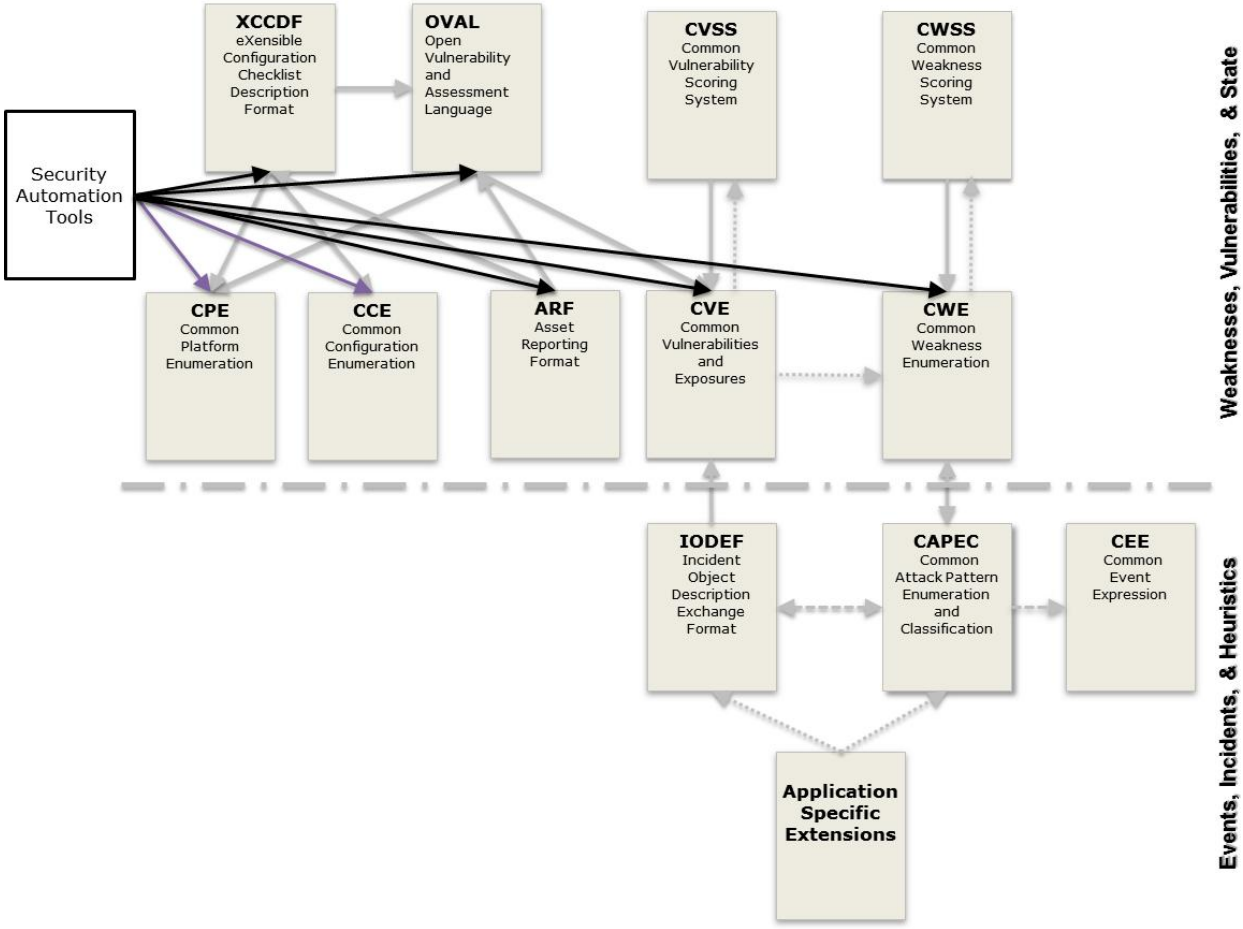

Figure 9 – Cybersecurity Assurance and Integrity Automation

A.1 Federal Desktop Core Configuration/United States Government Configuration Baseline.

The Federal Desktop Core Configuration (FDCC) and its replacement, the United States Government Configuration Baseline (USGCB), using the NIST Security Content Automation Protocol (SCAP) comprises specifications for organizing and expressing security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities.

The purpose of these two initiatives is to create security configuration baselines for ICT products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security.

The USGCB 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 six specifications: XCCDF, OVAL, CPE, CCE, CVE, and CVSS. These specifications are grouped into three categories: languages, enumerations, and vulnerability measurement and scoring systems.

SCAP implements 1) a specified format and nomenclature by which security software products communicate software flaw and security configuration information, and 2) specific software flaw and security configuration standard reference data known as SCAP content. Goals for SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content. Because many different SCAP contents are likely to emerge for diverse systems and levels of security, the structured tagging, discovery, and assurance verification of current schema are important requirements. The USGCB initiative creates content and guidance based on the SCAP specifications.

A.2 Vulnerability Information Portal Site, JVN

JVN stands for “Japan Vulnerability Notes” and provides vulnerability and related information on software used in Japan, with which it intends to contribute to the countermeasure to cyber threats. In order to enable application developers to use data through an open interface, JVN has adopted SCAP and contains local (domestic) information and international information, resulting in the JVN Security Content Automation Framework. Just like the National Vulnerability Database (NVD), each of the vulnerability information contains a CVE number, provides a CVSS score, and a CWS number. Moreover, the CPE name of the affected product is also provided.

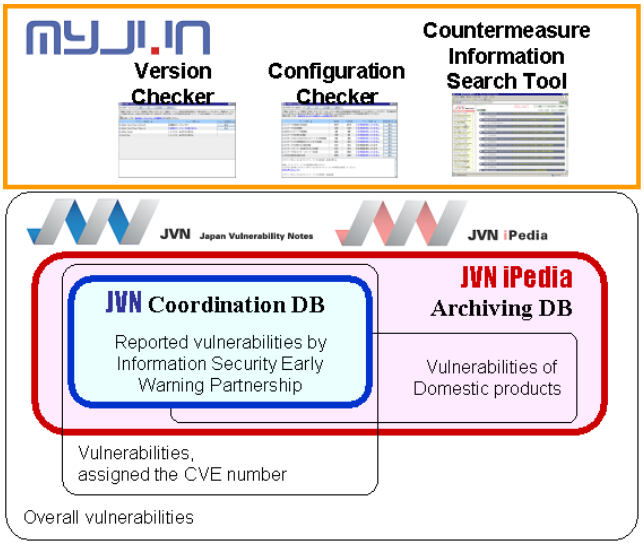

Figure 10 – Concept of JVN Security Content Automation Framework

The framework consists of three components: MyJVN, JVN, and JVN iPedia (see Figure 10), each of which is elaborated below.

MyJVN provides vulnerability countermeasure information via MyJVN API, a machine readable interface including Web APIs, and the MyJVN tools such as the Version Checker. It improves the usage of vulnerability countermeasure information stored in JVN and JVN iPedia by making it easier and more efficient for users to collect their target information through the services like customized filtering, auto searching and checklist creation. Also, "MyJVN Version Checker," a tool based on SCAP, allows people to easily check whether the software installed on their PC is the latest version.

JVN provides vulnerability countermeasure information and Japanese vendor status for reported vulnerabilities by "Information Security Early Warning Partnership"., which is a public-private partnership framework has been established to promote software product and web site security and prevent the damage to spread to the vast range of computers due to computer viruses or unauthorized access. When the vulnerability information is reported to IPA (Information-technology Promotion Agency, Japan) as the recipient body of this partnership, it is passed to the JPCERT/CC as a coordination body. JPCERT/CC specifies the affected software products and coordinates with developers. When solutions for vulnerability such as patches or software updates are available for users, the vulnerability details with developers' statements are published on JVN.

JVN iPedia provides vulnerability countermeasure information collected on software products, such as operating systems, applications, libraries and embedded systems, used in Japan. JVN aims to offer the vulnerability and countermeasure information to the public as soon as possible. A coordination body interacts with the vendors regarding when to disclose new reported vulnerabilities. The JVN iPedia mission on the other hand, aims to collect additional vulnerability and countermeasure information found on a daily basis on Japanese software products that are not released on JVN.

Users adopting standard formats such as RSS may enjoy a database that contains international and local information (see Figure 11). Among the three components, MyJVN works as a user interface, whose usability is facilitated with the tools and APIs elaborated in the next section.

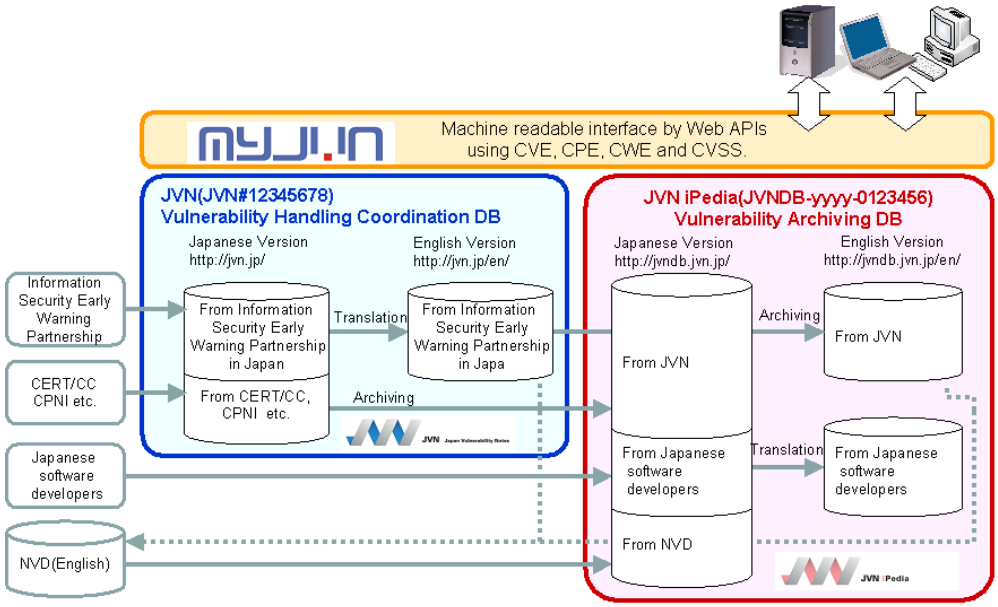

Figure 11 – Database with International and local information

MyJVN tools and API

The MyJVN tools are security tools based on SCAP that improve the usage of vulnerability countermeasure and information exchange environment for users. Currently, the major tools we offer are as follows:

Filtered Vulnerability Countermeasure Information Tool improves the usage of vulnerability countermeasure information stored in JVN and JVN iPedia by making it easier and more efficient for users to collect their target information through services like customized filtering by CPE.

Version Checker is an OVAL based on-line scanner that allows people to easily check whether the software installed on their PC is the latest version. With just one mouse click, people can check the versions of multiple software. The results are easy to understand: a tick mark signifies the latest version and a cross mark signifies an obsolete version. If the software is not the latest version, users can easily access the vendor's download website with just a few clicks. MyJVN Version Checker supports internet-related software products that were selected seeking cooperation from the software vendors.

MyJVN Security Configuration Checker is an XCCDF and OVAL based on-line scanner. It is a free, easy-to-use tool to assess Windows security configuration, including account policies such as the minimum password length, password expiration period, automatic turn-on of screensaver, the USB autorun feature, etc.

MyJVN API is a software interface to access and utilize vulnerability countermeasure information stored in JVN and JVN iPedia. To enable application developers to use data through an open interface, JVN iPedia has adopted SCAP, a set of standards for describing vulnerability countermeasure information. By using MyJVN API, any custom applications can access the data in JVN iPedia and various vulnerability management services can now efficiently utilize vulnerability countermeasure information.

Basic functions of MyJVN API are a filtered information service API and SCAP collaboration service API. The former API supports "Get list of products", "Get list of vulnerability overviews" etc., that are used by the Filtered Vulnerability Countermeasure Information Tool. The latter API

supports “Get list of OVAL definitions”, “Get data of OVAL definition” etc., that are used by the MyJVN Version Checker and the MyJVN Security Configuration Checker.