V1.0

ITU-T SG17 Tutorial
Geneva, 18 Sep 2009

Significant Cybersecurity Developments:

a global cybersecurity information exchange framework, plus Clouds, SmartGrid, and eHealth

Tony Rutkowski
Cybersecurity Rapporteur (ITU-T Q.4/17)

This presentation describes the extensive efforts within the ITU-T *Rapporteur Group on Cybersecurity* and its *Correspondence Group on the Trusted Exchange of Network Forensics* during Mar-Sep 2009 to assemble information about the current cybersecurity environment and steps proposed to assist in providing important cybersecurity capabilities.

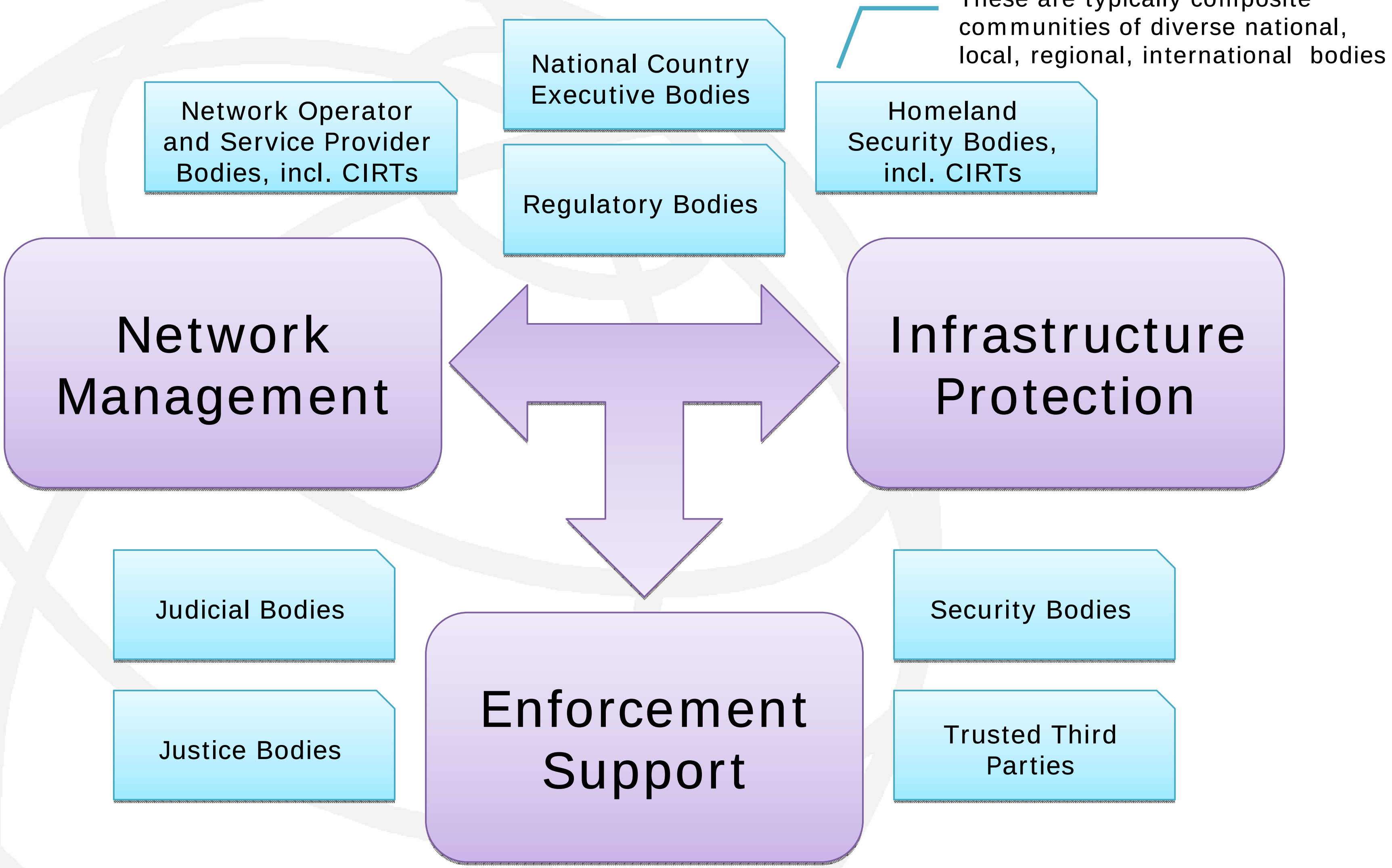
The core part of these capabilities is draft Rec. ITU-T X.cybex, *Global Cybersecurity Information Exchange Framework*

The work includes recent developments related to cybersecurity for Cloud infrastructure, SmartGrids and eHealth

Why Cyber Security Matters

- Network infrastructure/service providers and users are facing extraordinary levels of intentional and unintentional threats
  - As of July 2009, Spain’s Panda Networks was detecting 37 thousand new viruses, worms, Trojans, and other security threats per day
  - The totals have reached 30 million different varieties and are rapidly evolving
- The threats are growing exponentially
- The situation will get worse unless collective global action occurs on implementing infrastructure-based cyber security capabilities

Cybersecurity Forensics Convergence



These are typically composite communities of diverse national, local, regional, international bodies

National Country Executive Bodies
Network Operator and Service Provider Bodies, incl. CIRTs
Homeland Security Bodies, incl. CIRTs
Regulatory Bodies
Network Management
Infrastructure Protection
Judicial Bodies
Security Bodies
Enforcement Support
Justice Bodies
Trusted Third Parties

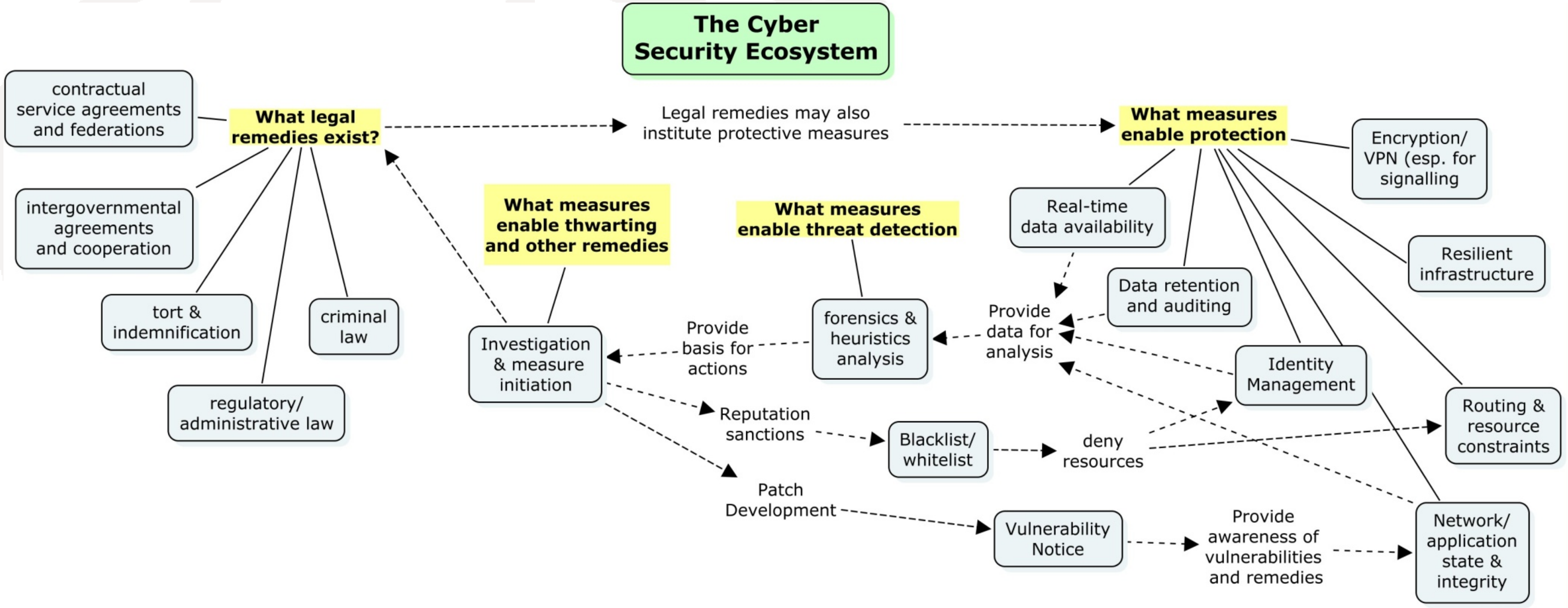
Network Forensics and Vulnerabilities Organizations

1 Global Intergovernmental
2 Global Non-Governmental
3 Regional Governmental
4 Regional and Other Non-Governmental
5 National Governments

http://www.ituwiki.com/Network_Forensic_and_Vulnerability_Organizations

TSB Director requested to keep current pursuant to WTSA Res. 58

The Cyber Security Ecosystem


The Cyber Security Ecosystem
contractual service agreements and federations
What legal remedies exist?
Legal remedies may also institute protective measures
What measures enable protection
Encryption/ VPN (esp. for signalling)
intergovernmental agreements and cooperation
tort & indemnification
criminal law
regulatory/ administrative law
What measures enable thwarting and other remedies
What measures enable threat detection
Real-time data availability
Resilient infrastructure
Data retention and auditing
Investigation & measure initiation
Provide basis for actions
forensics & heuristics analysis
Provide data for analysis
Identity Management
Reputation sanctions
Blacklist/ whitelist
deny resources
Routing & resource constraints
Patch Development
Vulnerability Notice
Provide awareness of vulnerabilities and remedies
Network/ application state & integrity

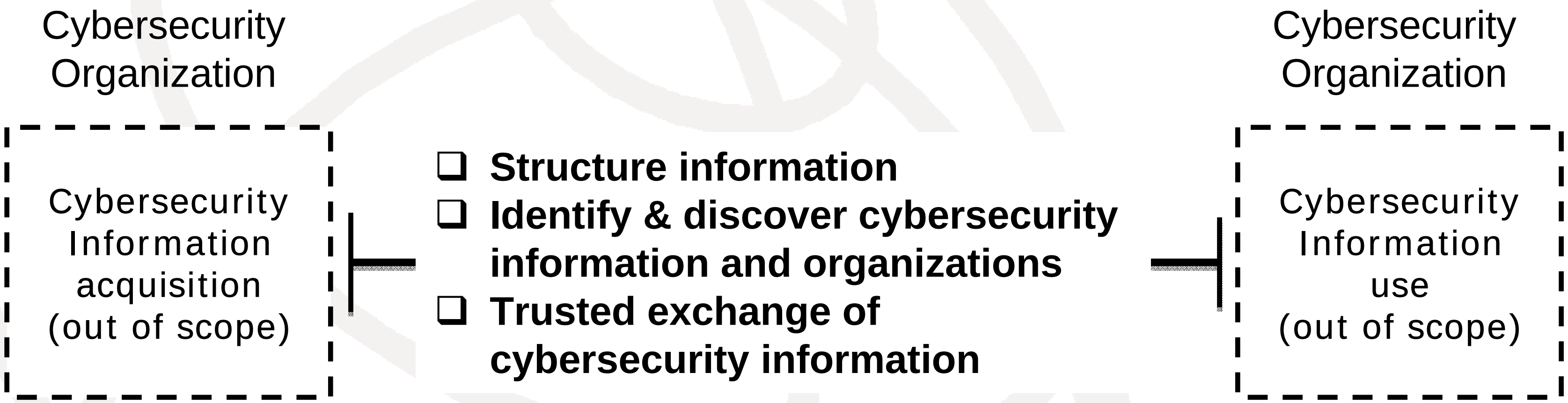
Trusted Information Exchange is critical to Cyber Security

- ❑ The “cybersecurity state” of equipment, software or network based systems, especially vulnerabilities – making security measureable
- ❑ Forensics related to incidents or events
- ❑ Heuristics and signatures gained from experienced events
- ❑ Parties who implement cybersecurity information exchange capabilities
- ❑ Specifications for the exchange of cybersecurity information, including modules, schemas, and assigned numbers
- ❑ The identities and trust attributes of all of the above

Why a global framework for exchanging cybersecurity information?

- ❑ Present environment is marked by “insularity”
- ❑ Enable global capabilities for the structured exchange of *cybersecurity information* by
  - – identifying and incorporating existing “best of breed” platform standards
  - – as necessary, making the existing standards more global and interoperable
- ❑ Move beyond guidelines and facilitate the scaling and broad implementation of core capabilities already developed within diverse cybersecurity communities

Focus on a basic model



Cybersecurity Organization

Cybersecurity Information acquisition (out of scope)

❑ Structure information

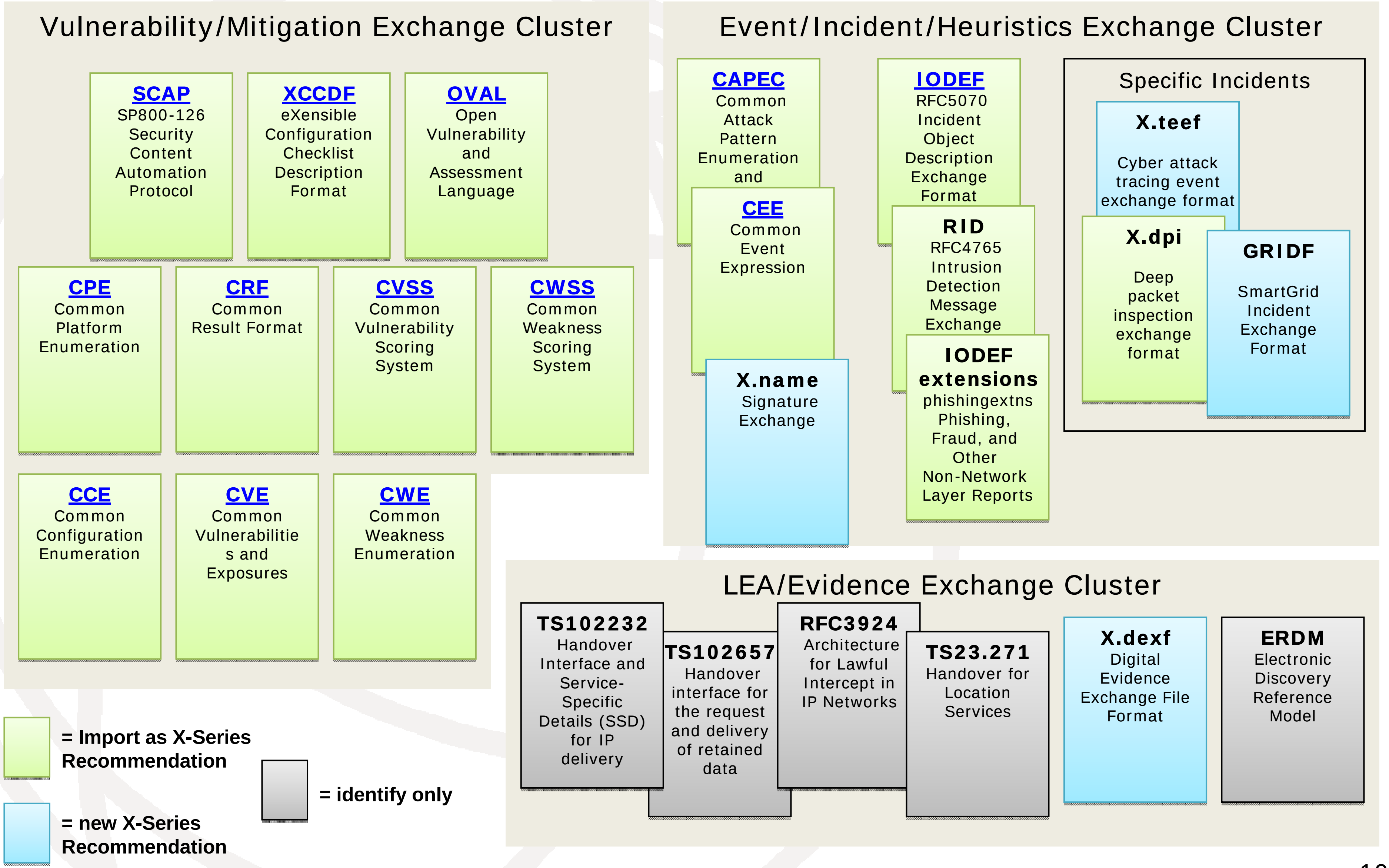
❑ Identify & discover cybersecurity information and organizations

❑ Trusted exchange of cybersecurity information

Cybersecurity Organization

Cybersecurity Information use (out of scope)

Structured Information



Vulnerability/Mitigation Exchange Cluster

SCAP SP800-126 Security Content Automation Protocol

XCCDF eXensible Configuration Checklist Description Format

OVAL Open Vulnerability and Assessment Language

CPE Common Platform Enumeration

CRF Common Result Format

CVSS Common Vulnerability Scoring System

CWSS Common Weakness Scoring System

CCE Common Configuration Enumeration

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

Event/Incident/Heuristics Exchange Cluster

CAPEC Common Attack Pattern Enumeration and

CEE Common Event Expression

X.name Signature Exchange

IODEF RFC5070 Incident Object Description Exchange Format

RID RFC4765 Intrusion Detection Message Exchange

IODEF extensions phishingextns Phishing, Fraud, and Other Non-Network Layer Reports

Specific Incidents

X.teef Cyber attack tracing event exchange format

X.dpi Deep packet inspection exchange format

GRIDF SmartGrid Incident Exchange Format

LEA/Evidence Exchange Cluster

TS102232 Handover Interface and Service-Specific Details (SSD) for IP delivery

TS102657 Handover interface for the request and delivery of retained data

RFC3924 Architecture for Lawful Intercept in IP Networks

TS23.271 Handover for Location Services

X.dexf Digital Evidence Exchange File Format

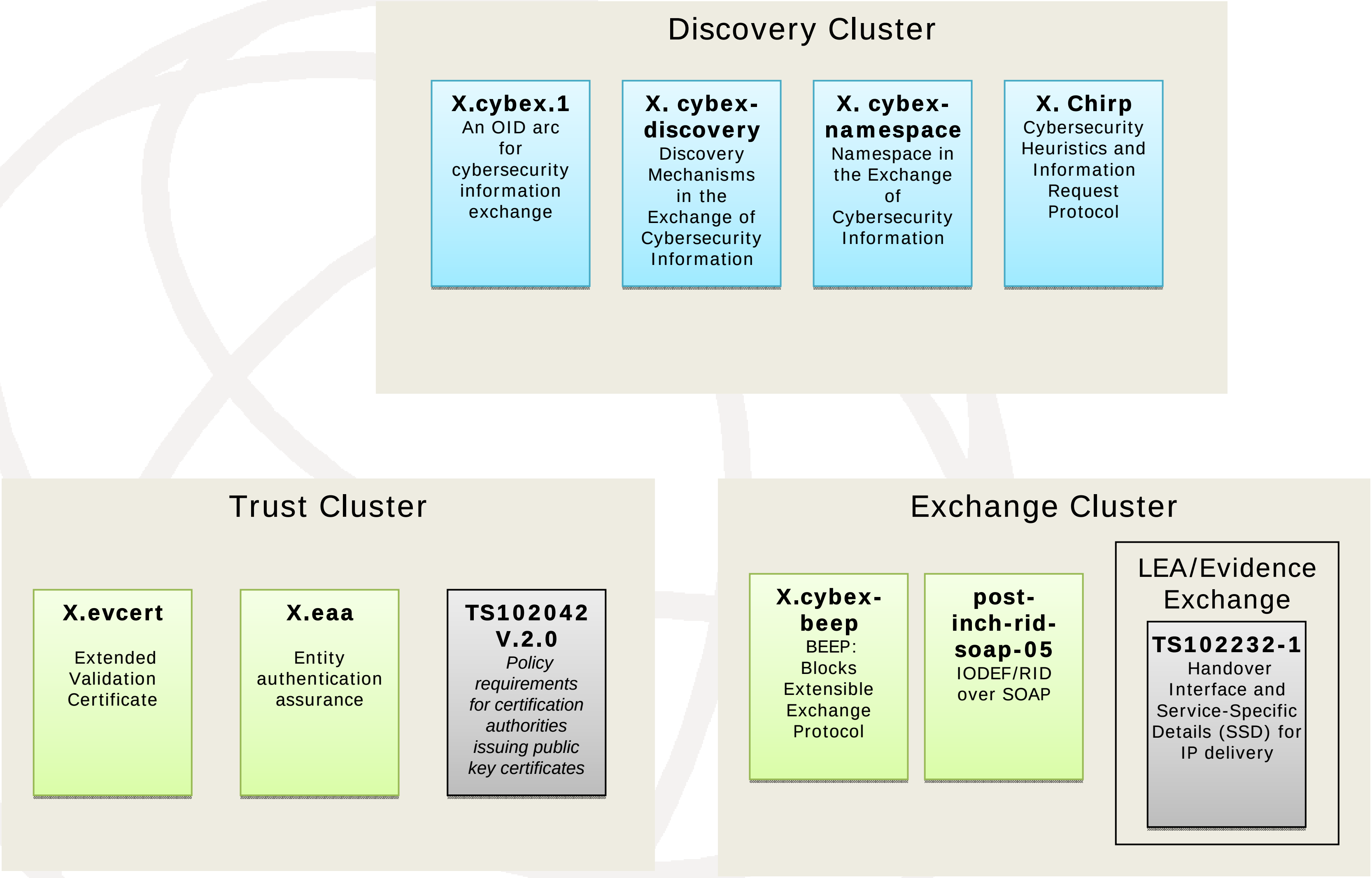
ERDM Electronic Discovery Reference Model

🟩 **= Import as X-Series Recommendation**

🟦 **= new X-Series Recommendation**

▨ **= identify only**

Discovery and Trusted Exchange



Discovery Cluster

X.cybex.1 An OID arc for cybersecurity information exchange

X. cybex-discovery Discovery Mechanisms in the Exchange of Cybersecurity Information

X. cybex-namespace Namespace in the Exchange of Cybersecurity Information

X. Chirp Cybersecurity Heuristics and Information Request Protocol

Trust Cluster

X.evcert Extended Validation Certificate

X.eaa Entity authentication assurance

TS102042 V.2.0 *Policy requirements for certification authorities issuing public key certificates*

Exchange Cluster

X.cybex-beep BEEP: Blocks Extensible Exchange Protocol

post-inch-rid-soap-05 IODEF/RID over SOAP

LEA/Evidence Exchange

TS102232-1 Handover Interface and Service-Specific Details (SSD) for IP delivery

Cybersecurity Requirements & Guidelines Proliferate

Generic Cybersecurity

ITU-T Q4/17

X.1205
Overview of cybersecurity

X.gopw
Guideline on preventing malicious code spreading in a data communication network

ISO SC27WG4

WD27032
(N7558)
Guidelines for cybersecurity

WD27033-1
(N7584)
Guidelines for Network security

WD27034
(N7564)
Application security

ITU-T Q4/17

X.sisfreq
Requirement for security information sharing

X.gpn
Mechanism and procedure for distributing policies for network security

ITU-T Q16/13

Y.2701
Next Generation Network security

ITU-T Q4/17

X.tsgf
Information security governance framework

ISO SC27WG1

WD27014
(N7820)
information security governance framework

Incident Forensics

ITU-T Q4/17

X.1056
Security Incident Management for telecommunications organizations

ISO SC27WG4

WD27035
(N7566)
Information Security Incident Management

X.bots
Framework for botnet detection and response

ITU-T Q4/17

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

ITU-T Q17/13

Y.dpireq
NGN deep packet inspection requirements

ISO SC27WG4

WD27037
(N7570)
Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Vulnerability Exchange

ITU-T Q4/17

X.1206
automatic notification of security related information and dissemination of updates

ISO SC27WG3

WD29147
(N7901)
Responsible Vulnerability disclosure

ISO SC27WG1

WD27010-2
(N7607)
Communication and Alerting Protocol and Mechanisms

LEA Forensics

TS102656
Retained Data Requirements

ETSI TC LI

TS101331
Requirements of Law Enforcement Agencies

Cloud Cybersecurity

- ❑ a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction
- ❑ Cloud Service Models
  - – Software as a Service (SaaS)
  - – Platform as a Service (PaaS)
  - – Infrastructure as a Service (IaaS)
- ❑ Cloud Deployment Models
  - – Private
  - – Community
  - – Public
  - – Hybrid
- ❑ An extremely fast moving development
  - – National agencies are assessing the environment
  - – Cybersecurity/hypervisors/legal are major challenges
  - – http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
- ❑ Cloud Security Alliance recently formed
  - – www.cloudsecurityalliance.org/
- ❑ CYBEX intended to be “cloud capable”

SmartGrid Cybersecurity

- ❑ Marriage of electric grid and “intelligence infrastructure”
- ❑ A major focus of recent Global Standards Collaboration #14 July meeting
- ❑ Entwined with ITU-T NID and Climate Change initiatives
- ❑ An extremely fast moving development
  - – National/regional agencies are assessing the environment
  - – Cybersecurity is a major challenge
- ❑ NIST CyberSecurity Coordination Task Group
  - – http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
  - – Subset of Smart Grid Interoperability Standards Project
  - – Major announcements at Grid Week (next week)
- ❑ CYBEX intended to be “SmartGrid capable”

eHealth Cybersecurity

- Marriage of Health IT and "intelligence infrastructure"
- Entwined with ITU-T biohealth and biometrics standards work
- An extremely fast moving development
  - National/regional agencies are assessing the environment
  - Cybersecurity is a major challenge
- ISO has TC215 –Health Informatics, WG4 - Security
- ETSI has an eHealth Technical Committee and Specialist Task Force 355
- New US Health IT Standards Committee
  - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1271&parentname=CommunityPage&parentid=6&mode=2
  - Security Workgroup
- eHealth cybersecurity focus is at very initial stages and remains relatively primitive
- CYBEX intended to be "eHealth capable"