Cyber Security Measurement & Management Architecture

Knowledge Repositories

Asset Definition
CPE, OVAL, SWID

Configuration Guidance
XCCDF, OVAL, CCE, OCIL, CCSS

Vulnerability Alert
CVE, CWE, OVAL, CVSS, CVRF

Threat Alert
CVE, CWE, CVSS, CAPEC, MAEC, CybOX, STIX

Indicator Sharing
STIX, CVE, CPE, MAEC, CEE, CybOX, IODEF

Incident Report
CYBEX, CWE, STIX, OVAL, CVE, CPE, CVSS, MAEC, CEE, CWSS, CybOX, IODEF

Development & Sustainment Security Management Processes

OVAL, XCCDF, CPE, OCIL

System Assurance Guidance/ Mandates/ Requirements

CWE, CAPEC, SBVR, MAEC

Asset Inventory
CPE, OVAL, SWID

Configuration Guidance Analysis
CCE, OVAL, OCIL, XCCDF, CPE, SWID, CCSS

Vulnerability Analysis
CVE, CWE, CVSS, CCE, OVAL, OCIL, XCCDF, CPE, CWSS, SWID

Threat Analysis
CVE, CWE, CVSS, CCE, OVAL, OCIL, XCCDF, CPE, CAPEC, MAEC, CybOX, SWID, STIX

Intrusion Detection
CVE, CWE, CVSS, CCE, OVAL, OCIL, XCCDF, CPE, CAPEC, MAEC, CEE, CybOX, SWID, STIX

Incident Management

Assessment of System Development, Integration, Sustainment Activities, and Certification & Accreditation

INTERNET

Router

DMZ

Firewall

INTRANET

Web Servers

Application Servers

Database Systems

DNS Server

Mail Server

Web Servers

Desktop Systems

Desktop Systems

Desktop Systems

Desktop Systems

Enterprise IT Change Management
CVE, CWE, CVSS, CCE, OVAL, XCCDF, CPE, CAPEC, MAEC, CEE, CWSS, CCSS, SWID, CybOX

Centralized Reporting
CVE, CWE, CVSS, CCE, OVAL, XCCDF, CPE, CAPEC, MAEC, CEE, CWSS, CCSS, SWID, CybOX