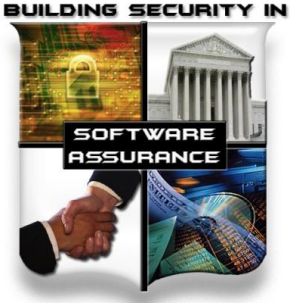


Software Assurance (SwA)

Common Weakness Scoring System (CWSS):

Using CWE to provide consistent measures for prioritizing risk mitigation efforts

CWSS at cwe.mitre.org

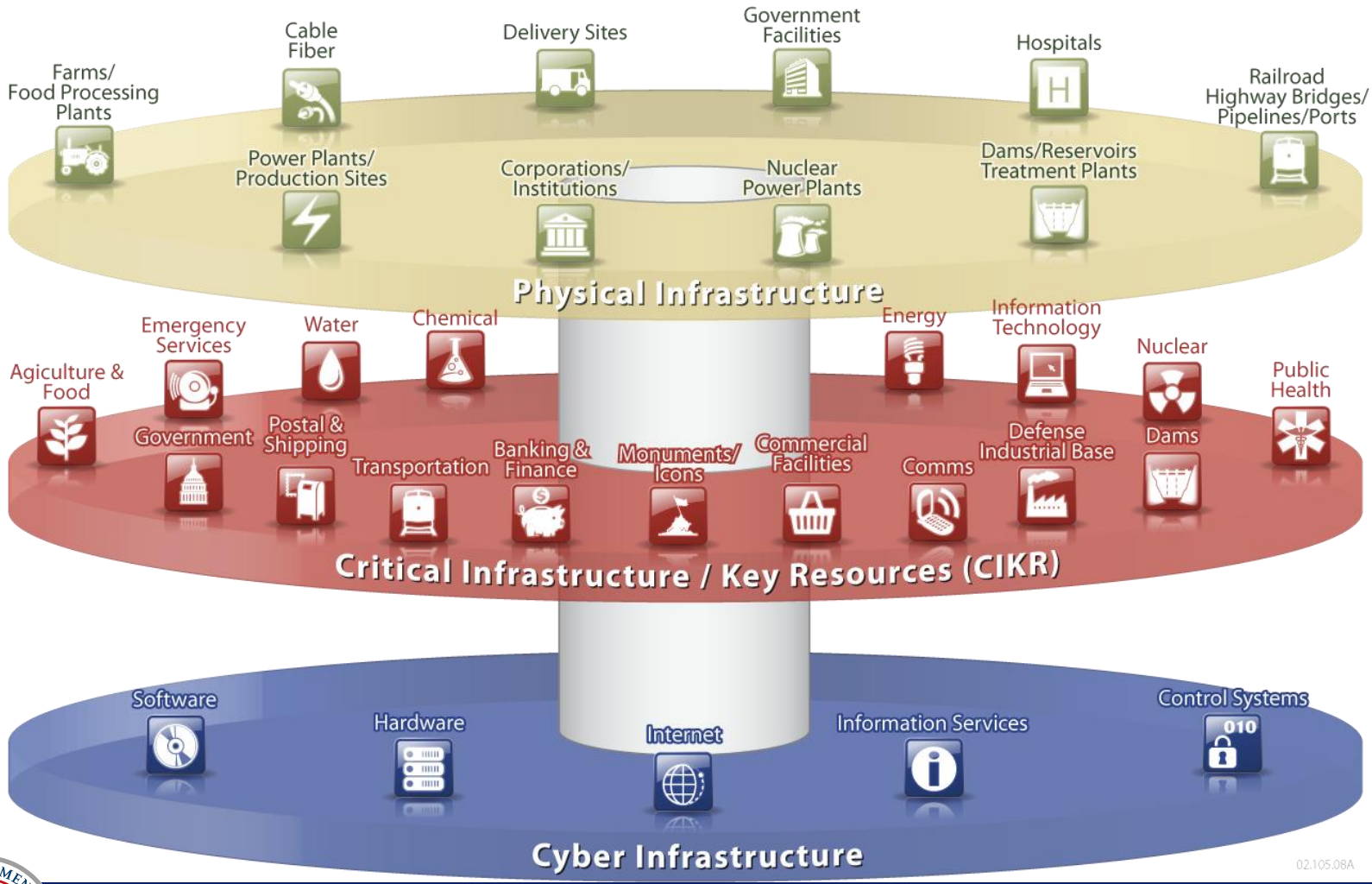
March 3, 2011

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Office of the Assistant Secretary for
Cybersecurity and Communications

Homeland Security

Interdependencies Between Physical & Cyber Infrastructures: Requires Convergence of Safety, Security and Dependability

-- Need for secure software applications

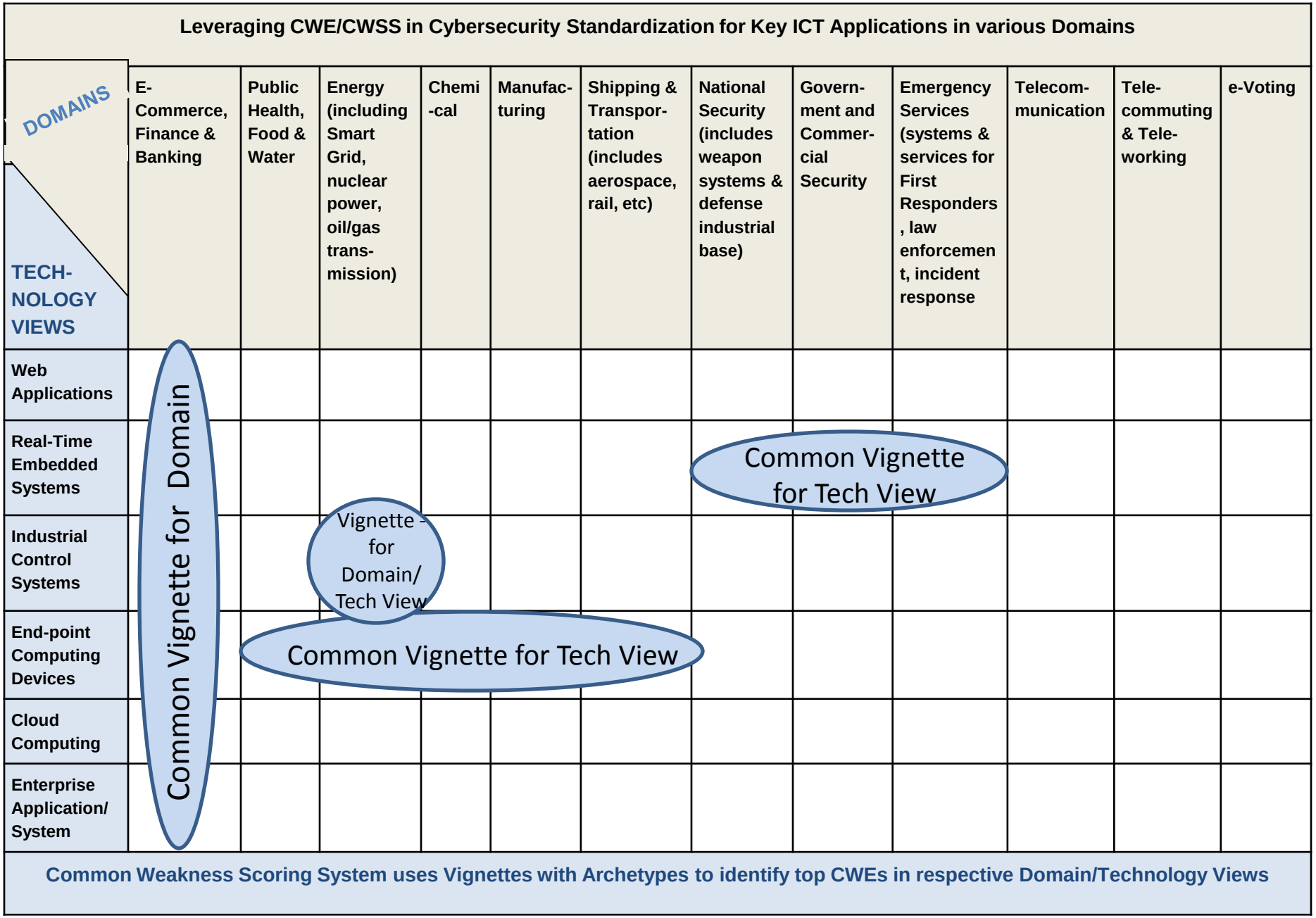


Technologies Subject to Exploitation:
Providing Context for the Priority of Common Weaknesses

Technology Views	Archetypes
Web Application	Web browser, web-server, web-based applications and services, etc.
Industrial Control System	SCADA, process control systems, etc
Embedded System	Embedded Device, Programmable logic controller, implanted medical devices, avionics package
End-point Computing Device	Smart phone, laptop, and other remote devices that leave the enterprise and/or connect remotely to the enterprise
Cloud Computing	Software-enabled capabilities and services (either installed locally or offered via hosted services/cloud computing), such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)
Enterprise Application/System	includes Databases, Operating Systems, office products (such as word processing, spreadsheets, etc)

Domains	Description
E-Commerce	The use of the Internet or other computer networks for the sale of products and services, typically using on-line capabilities.
Banking & Finance	Financial services, including banks, stock exchanges, brokers, investment companies, financial advisors, and government regulatory agencies.
Public Health, Food & Water	Health care, medical encoding and billing, patient information/data, critical or emergency care, medical devices (implantable, partially embedded, patient care), drug development and distribution, food processing, clean water treatment and distribution (including dams and processing facilities), etc.
Energy	Smart Grid (electrical network through a large region, using digital technology for monitoring or control), nuclear power stations, oil and gas transmission, etc.
Chemical	Chemical processing and distribution, etc.
Manufacturing	Plants and distribution channels, supply chain, etc.
Shipping & Transportation	Aerospace systems (such as safety-critical ground aviation systems, on-board avionics, etc), shipping systems, rail systems, etc.
National Security	National security systems (including networks and weapon systems), defense industrial base, etc.
Government and Commercial Security	Homeland Security systems, commercial security systems, etc
Emergency Services	Systems and services that support for First Responders, incident management and response, law enforcement, and emergency services for citizens, etc.
Telecommunications	Cellular services, land lines, VOIP, cable & fiber networks, etc.
Telecommuting & Teleworking	Support for employees to have remote access to internal business networks and capabilities.
eVoting	Electronic voting systems, as used within state-run elections, shareholder meetings, etc.

Common Weakness Scoring System (CWSS) Vignettes



Vignettes and Business Value Context

Vignette provides a shareable, formalized way to define a particular environment within a business domain:

- includes the role that software archetypes play within that environment, and an organization's priorities with respect to software security.
- Identifies essential resources and capabilities, as well as their importance relative to security principles such as confidentiality, integrity, and availability. For example, in an e-commerce context, 99.999% uptime may be a strong business requirement that drives the interpretation of the severity of discovered weaknesses.
- Allows CWSS to support diverse audiences who may have different requirements for how to prioritize weaknesses. CWSS scoring occurs within the context of a vignette.

Business Value Context (BVC) contains three main parts:

(1) a general description of the security-relevant archetypes, assets, and interfaces that are of concern to the business domain

(2) the security priorities of the business domain with respect to the potential outcomes that could occur if those archetypes are successfully attacked.

(3) a Technical Impact, in which the business domain's security concerns are linked with the potential technical impact that could occur if weaknesses are discovered and exploited.

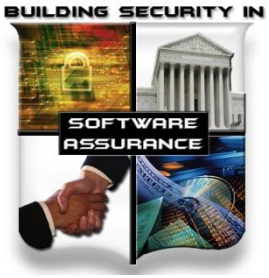
Vignettes and Business Value Context

Domain	Vignette	Description	Archetypes	Business Value Context (BVC)
e-commerce	Web-based Retail Provider	Internet-facing, E-commerce provider of retail goods or services. Data-centric - Database containing PII, credit card numbers, and inventory.	Database, Web client/server, General-purpose OS	Confidentiality essential from a financial PII perspective, identity PII usually less important. PCI compliance a factor. Security incidents might have organizational impacts including financial loss, legal liability, compliance/regulatory concerns, and reputation/brand damage.
Finance	Financial Trading / Transactional	Financial trading system supporting high-volume, high-speed transactions.	N-tier distributed, J2EE and supporting frameworks, Transactional engine	High on integrity - transactions should not be modified. Availability also very high - if system goes down, financial trading can stop and critical transactions are not processed.

Vignettes and Business Value Context

Domain	Vignette	Description	Archetypes	Business Value Context (BVC)
Public Health	Human Medical Devices	Medical devices - "implantable" or "partially embedded" in humans, as well as usage in clinic or hospital environments ("patient care" devices.) Includes items such as pacemakers, automatic drug delivery, activity monitors. Control or monitoring of the device might be performed by smartphones. The devices are not in a physically secured environment.	Web-based monitoring and control, General-purpose OS, Smartphone, Embedded Device	Power consumption and privacy a concern. Key management important. Must balance ease-of-access during emergency care with patient privacy and day-to-day security. Availability is essential - failure of the device could lead to illness or death. Devices are not in a physically secured environment.
Smart Grid	Smart Meters	Meter that records electrical consumption and communicates this information to the supplier on a regular basis.	Web Applications, Real-Time Embedded System, Process Control System, End-point Computing Device	Confidentiality of customer energy usage statistics is important - could be used for marketing or illegal purposes. For example, hourly usage statistics could be useful for monitoring activities. Integrity of metering data is important because of the financial impact on stakeholders (consumers manipulating energy costs). Availability typically is not needed for real-time; other avenues exist if communications are disrupted (e.g., site visit).

Next SwA Working Group 28-30 June 2011 at MITRE, McLean, VA



SOFTWARE ASSURANCE FORUM

"Building Security In"

https://buildsecurityin.us-cert.gov/swa

See CWSS & Top 25 CWE at cwe.mitre.org

Homeland Security

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126
LinkedIn SwA Mega-Community