Software Security Assurance: Software Supply Chain Risk Management

June 15, 2011

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Public/Private Collaboration Efforts for Software Supply Chain Risk Management

Next SwA Working Groups meet 28-30 June 2011 at MITRE, McLean, VA
Interdependencies Between Physical & Cyber Infrastructures Requires Convergence of Safety, Security and Dependability

In an era riddled with asymmetric cyber attacks, claims about system reliability and safety must include provisions for built-in security of the enabling software.

High Reliability and Human Safety Critical Software
Cyber Infrastructure represents the convergence of information technology and communications systems, is inherent to nearly every aspect of modern life.

Illustrative examples only -- not all inclusive.
Today Everything’s Connected

Your System is attackable...

When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…
Interdependencies Between Physical & Cyber Infrastructures: Requires Convergence of Safety, Security and Dependability

-- Need for secure software applications
Software Security Assurance: Not just a good idea

• Many people responsible for protecting most critical infrastructure facilities have felt comfortable about security of their systems.
  – Facilities rely on industrial control systems (ICS) -- custom-built suites of systems that control essential mechanical functions of power grids, processing plants, etc -- usually not connected to the Internet, also known as "air-gapped."
  – Many industry owners, operators and regulators believed that this security model provided an infallible, invulnerable barrier to malicious cyber attacks from criminals and advanced persistent threat (APT) adversaries.

• National Defense Authorization Act (NDAA) -- which included a focus on software security (in Section 932, Strategy on Computer Software Assurance) -- serves as first cybersecurity law of 2011 and requires the U.S. Dept of Defense to develop a strategy for ensuring the security of software applications.

• Software Security Assurance, a set of practices for ensuring proactive application security, is key to making applications compliant with this new law.

NRC Regulatory Guidance on Cyber Security

  - Directly relates to current NRC guidance on cyber security in the supply chain and SDLC of an ICS regulated by the agency.
  - Section C.12.2 “Supply Chain Protection” control drill down to the vendor level with requirements accountability for the RG 5.71 control baseline (Appendices B&C).
  - Section C.12.3 “Trustworthiness” requires developers employ software quality and validation methods to minimize flawed or malformed software; requires all tools to undergo commercial certification process
  - Section C.12.5 “Developer Security Testing”

Understanding the Threat and Controlling the Attack

One who knows the enemy and knows himself will not be endangered in a hundred engagements.

One who does not know the enemy but knows himself will sometimes be victorious; sometimes meet with defeat.

One who knows neither the enemy nor himself will invariably be defeated in every engagement.

■ The Art of War, Sun Tzu

An appropriate defense can only be established if one knows its weaknesses and how it will be attacked; thus controlling attack surface/vectors

■ Software Assurance Forum, Joe Jarzombek
Buffer Overflow (CWE-120) Exploit (CAPEC-123)

SQL Injection (CWE-89) Exploit (CAPEC-66)

Security Feature
If the weaknesses in software were as easy to spot and their impact as obvious as…
Leveraging Vignettes in Cyber Security Standardization for Key ICT Applications in various Domains

Common Weakness Risk Assessment Framework uses Vignettes with Archetypes to identify top CWEs in respective Domain/Technology Groups.
Common Weakness Risk Analysis Framework (CWRAF)

- CWRAF enables organizations to apply the Common Weakness Scoring System (CWSS)
  - using specialized, targeted scenarios ("vignettes")
  - that identify the business value context of deployed applications
  - to prioritize those software weaknesses (CWE) that are most relevant to their own businesses, missions, and deployed technologies.

- CWRAF:
  - includes a mechanism for measuring risk of weaknesses in a way that is closely linked with the risk to the business or mission;
  - supports the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the business or mission;
  - can be used by consumers to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance; and
  - allows users to create custom Top-N lists to rank classes of weaknesses independent of any particular software package, to prioritize them relative to each other (e.g., "buffer overflows are higher priority than memory leaks"). This "Top-N list" approach is also used by the CWE/SANS Top 25, OWASP Top Ten, etc..

CWRAF - [http://cwe.mitre.org/cwraf/index.html](http://cwe.mitre.org/cwraf/index.html)

CWRAF is a part of the CWE project, co-sponsored by the Software Assurance program in the National Cyber Security Division of the U.S. Department of Homeland Security. Community review/feedback of CWRAF & CWSS should be sent to cwss@mitre.org.
CWRAF/CWSS Provides Risk Prioritization for CWE throughout Software Life Cycle

• Enables education and training to provide specific practices for eliminating software fault patterns;

• Enables developers to mitigate top risks attributable to exploitable software;

• Enables testing organizations to use suite of test tools & methods (with CWE Coverage Claims Representation) that cover applicable concerns;

• Enables users and operation organizations to deploy and use software that is more resilient and secure;

• Enables procurement organizations to specify software security expectations through acquisition of software and services.
Security is a Requisite Quality Attribute: Vulnerable Software Enables Exploitation

- Rather than attempt to break or defeat network or system security, hackers are opting to target application software to circumvent security controls.

  - **75% of hacks occurred at application level**
    - “90% of software attacks were aimed at application layer” (Gartner & Symantec, June 2006)

  - Most exploitable software vulnerabilities are attributable to non-secure coding practices (and not identified in testing).

- Functional correctness must be exhibited even when software is subjected to abnormal and hostile conditions.

In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity & safety must include provisions for built-in security of the enabling software.
Critical Considerations

Software is the core constituent of modern products and services – it enables functionality and business operations.

Dramatic increase in mission risk due to increasing:
- Software dependence and system interdependence (weakest link syndrome)
- Software Size & Complexity (obscures intent and precludes exhaustive test)
- Outsourcing and use of un-vetted software supply chain (COTS & custom)
- Attack sophistication (easing exploitation)
- Reuse (unintended consequences increasing number of vulnerable targets)
- Number of vulnerabilities & incidents with threats targeting software
- Risk of Asymmetric Attack and Threats

Increasing awareness and concern

Software and the processes for acquiring and developing software represent a material weakness.
Software Assurance Addresses Exploitable Software: Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of “intent”

EXPLOITABLE SOFTWARE

Defects

Unintentional Vulnerabilities

Intentional Vulnerabilities

Malware

‘High quality’ can reduce security flaws attributable to defects; yet traditional S/W quality assurance does not address intentional malicious behavior in software

*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)

Committee on National Security Systems (CNSS) definition:
Software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner.
DHS Software Assurance Program Overview

- Program established in response to the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:
  “DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development.”

- DHS Program goals promote the **security and resilience** of software across the development, acquisition, and operational life cycle

- DHS Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities or malicious logic exist in the software, either intentionally or unintentionally inserted,
  - **Dependability (Correct and Predictable Execution)** - Justifiable confidence that software, when executed, functions as intended,
  - **Survivability** - If compromised, damage to the software will be minimized; it will recover quickly to an acceptable level of operating capacity; it’s ‘rugged’;
  - **Conformance** – Planned, systematic set of multi-disciplinary activities that ensure processes/products conform to requirements, standards/procedures.

See Wikipedia.org for “Software Assurance” - CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006, defines Software Assurance as: "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner". 
Software Assurance Forum & Working Groups*

... encourage the production, evaluation and acquisition of more secure and resilient software through targeting:

<table>
<thead>
<tr>
<th>People</th>
<th>Processes</th>
<th>Technology</th>
<th>Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers and users education &amp; training</td>
<td>Sound practices, standards, &amp; practical guidelines for secure software development</td>
<td>Security test criteria, measurement, diagnostic tools, common languages &amp; enumerations, SwA Research &amp; Development</td>
<td>Software security improvements through due-diligence questions, specs and guidelines for acquisitions/outsourcing</td>
</tr>
</tbody>
</table>

**Products and Contributions**

- Build Security In - https://buildsecurityin.us-cert.gov and SwA community resources & info clearinghouse
- SwA Common Body of Knowledge (CBK) & Glossary
- Organization of SwSys Security Principles/Guidelines
- SwA Developers' Guide on Security-Enhancing SDLC
- SwA Curriculum Project: Masters and Undergraduate
- Software Security Assurance State of the Art Report
- Systems Assurance Guide (via DoD and NDIA)
- Practical Measurement Framework for SwA/InfoSec
- Making the Business Case for Software Assurance
- SwA Metrics & Tool Evaluation (with NIST)
- SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG
- NIST Special Pub 500 Series on SwA Tools
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration (CAPEC)
- Malware Attribute Enumeration and Characterization
- SwA in Acquisition: Mitigating Risks to Enterprise
- Software Project Management for SwA SOAR

* SwA Forum is part of Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides legal framework for participation.
SwA Collaboration for Content & Peer Review

BSI https://buildsecurityin.us-cert.gov focuses on making Software Security a normal part of Software Engineering

SwA Community Resources and Information Clearinghouse (CRIC)

https://buildsecurityin.us-cert.gov/swa/ focuses on all contributing disciplines, practices and methodologies that advance risk mitigation efforts to enable greater resilience of software/cyber assets.

The SwA CRIC provides a primary resource for SwA Working Groups.

Where applicable, SwA CRIC & BSI provide relevant links to each other.
Software Assurance Curriculum Project

- **Vol I: Master of Software Assurance Reference Curriculum**
  
  In Dec 2010 the IEEE Computer Society and the ACM recognized the Master of Software Assurance (MSwA) Reference Curriculum as a certified master’s degree program in SwA — the first curriculum to focus on assuring the functionality, dependability, and security of software and systems.

- **Vol II: SwA Undergraduate Course Outlines**
  
  see [www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm](http://www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm) to download the PDF version of the report CMU/SEI-2010-TR-019

- **Vol III: Master of SwA Course Syllabi**

- **Vol IV: Community College Education**
  
  - To facilitate implementation, the MSwA project team is offering assistance, free of charge, to educational institutions looking to launch an MSwA degree program.
  - For more information on SwA Curriculum Project and MSwA, go to [https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html](https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html).
Software Assurance (SwA) Pocket Guide Series

SwA in Acquisition & Outsourcing
• Software Assurance in Acquisition and Contract Language
• Software Supply Chain Risk Management and Due-Diligence

SwA in Development
• Integrating Security into the Software Development Life Cycle
• Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
• Risk-based Software Security Testing
• Requirements and Analysis for Secure Software
• Architecture and Design Considerations for Secure Software
• Secure Coding and Software Construction
• Security Considerations for Technologies, Methodologies & Languages

SwA Life Cycle Support
• SwA in Education, Training and Certification
• Secure Software Distribution, Deployment, and Operations
• Code Transparency & Software Labels
• Assurance Case Management
• Secure Software Environment and Assurance EcoSystem

SwA Measurement and Information Needs
• Making Software Security Measurable
• Practical Measurement Framework for SwA and InfoSec
• SwA Business Case and Return on Investment

SwA Pocket Guides and SwA-related documents are collaboratively developed with peer review; they are subject to update and are freely available for download via the DHS Software Assurance Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa (see SwA Resources)
IT/software security risk landscape is a convergence between “defense in depth” and “defense in breadth”

Enterprise Risk Management and Governance are security motivators

Acquisition could be considered the beginning of the lifecycle; more than development

“In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains.”

– Dan Geer, CISO In-Q-Tel

Software Assurance provides a focus for:
-- Secure Software Components,
-- Security in the Software Life Cycle,
-- Software Security in Services, and
-- Software Supply Chain Risk Management
“Supply chain introduces risks to American society that relies on Federal Government for essential information and services.”

30 Sep 2005 changes to Federal Acquisition Regulation (FAR) focus on IT Security

Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

Risk Management (Enterprise <=> Project): Shared Processes & Practices // Different Focuses

**Enterprise-Level:**
- Regulatory compliance
- Changing threat environment
- Business Case

**Program/Project-Level:**
- Cost
- Schedule
- Performance

Software Supply Chain Risk Management traverses enterprise and program/project interests
Assurance Challenges in Mitigating Software Supply Chain Risks

- Complexity hampers our ability to determine and predict code behavior; so any “assurance” claims for security/safety-critical applications are limited.

- Without adequate diagnostic capabilities and commonly recognized standards from which to benchmark process capabilities and assert claims about the assurance of products, systems and services, the “provenance and pedigree of supply chain actors” become a more dominant consideration for security/safety-critical applications:
  - Enterprises and Consumers lack requisite transparency for more informed decision-making for mitigating risks;
  - Favoring domestic suppliers does not necessarily address ‘assurance’ in terms of capabilities to deliver secure/safe components, systems or software-reliant services.

- Several needs arise:
  - Need internationally recognized standards to support processes and provide transparency for more informed decision-making for mitigating enterprise risks.
  - Need ‘Assurance’ to be explicitly addressed in standards & capability benchmarking models for organizations involved with security/safety-critical applications.
  - Need more comprehensive diagnostic capabilities to provide sufficient evidence that “code behavior” can be well understood to not possess exploitable or malicious constructs.
  - Need rating schemes for software products and supplier capabilities.
25 Mar 2010 DoD Directive-Type Memorandum (DTM) 09-016 – Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems

**Policy.** It is DoD policy that:

- Supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

**SCRM.** The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport).

**Supply chain risk.** The risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications.
Major pipelines for IT/Software Supply Chain

1. From country where manufactured
   • to a certified domestic distributor to domestic end-user, or
   • through a certified distributor in a second country to domestic end-user

2. From country of origin
   • to online auction site (such as eBay or similar) to end-user
   • to distributor or retailer with unknown credentials to end-user

3. In most cases, IT/software is manufactured/produced by a non-vetted or uncertified supplier (especially for software) to domestic end-user

4. Transparency of supply chain complicated through re-supply of integrators, VARs, and service providers

US Government Contracting Process

Government or Govt. Contractor

(order placed)

GSA Approved IT Vendor

1st Sub-Contractor

2nd Sub-Contractor

3rd Sub-Contractor

Equipment Distributor

(drop ships as GSA Vendor)
The New Issue is Virtual Security

- In addition to physical security, we now worry about cyber risks:
  - Theft of intellectual property
  - Fake or counterfeit products
  - Import/export of strong encryption
  - IT/software with deliberately embedded malicious functionality
    - Logic bombs and self-modifying code
    - Other “added features” like key loggers
    - Deliberately hidden back doors for unauthorized remote access
  - Exploitable IT/software from suppliers with poor security practices
    - Failure to use manufacturing processes/capabilities to design and build secure products (no malicious intent) in delivering exploitable products
    - Re-suppliers (VARs, integrators, and service providers) often lack incentives and capabilities to adequately check content of sub-contracted and outsourced IT/software products

- IT/software security laws, policies, & standards are immature

Supply Chain Risk Management (SCRM) processes, tools and techniques:

Numerous SCRM processes, tools and techniques facilitate the implementation of SCRM USG-wide. Departments and Agencies shall adopt and tailor these recommended SCRM processes, tools, and techniques, and apply them to the procurement and operation of mission critical elements within NSS, to include those which:

- Control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including commercial elements or sub-elements.
- Detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit elements or malicious functions.
- Develop requirements or capabilities to detect the occurrence of vulnerabilities within custom and commodity hardware and software through enhanced test and evaluation.
SCRM processes, tools and techniques:

- Enhance security through the implementation of system security engineering (e.g. criticality analysis and defensive engineering practices) throughout the system life cycle.

- Optimize acquisition and contracting to define requirements and source selection criteria that reduce supply chain risk, give preference to vendors that minimize supply chain risk in verifiable ways, and evaluate security equally with other desirable factors, such as low cost, rapid deployment, or new features.

- Implement acquisition processes to document and monitor risk mitigation methods and requirements and provide for the update of documentation throughout the system lifecycle.
Best Practices, Tools and Techniques References

General SCRM References

The following documents provide systems security engineering guidance and detailed risk management best practice for use in commercial or government systems.


SCRM References from the Department of Defense

The following documents describe SCRM best practice for NSS, provide guidance on the successful implementation of SCRM pilots that incorporate all-source threat information, summarize the DoD pilot experience, and identify trusted suppliers of integrated circuits as accredited by the Defense Microelectronic Agency.


Draft Comprehensive National Cybersecurity Initiative (CNCI) DoD Supply Chain Risk Management (SCRM) Pilot Program Report, November 30, 2010


SCRM References from the Department of Homeland Security

The following documents and the assessment tool provide guidance for civilian Departments and agencies guidance for the successful implementation of a SCRM pilot. Used with the NISTIR 7622, which identifies key practices, the following documents enable the development and operation of systems to manage supply chain risks.

- Concept of Operations for the Civilian Agency Pilot Program (CAPP)
- Template for a SCRM Pilot Plan of Action and Milestones
- SCRM Capability Assessment Tool
Best Practices, Tools and Techniques References

Software Assurance Community documents from Software.Assurance@dhs.gov

Software Assurance in Acquisition and Contract Language (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html#acquisition)

Software Supply Chain Risk Management and Due Diligence (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html#acquisition)


Best Practices, Tools and Techniques References

Industry Standards for SCRM
- EIA-4899 - Standard for Preparing an Electronic Component Management Plan
- IDEA-STD-1010 – Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook
- SAE-AS9120 – Quality Management Systems for Aerospace Product Distributors
- SAE-AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition

Federal IT Security References
The following documents provide a foundation of federal information technology security practices or provide detailed guidance specific to managing risks inherent in the information technology product or services supply chain.

- NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009 (includes updates as of 05-01-2010).
We are engaged with many parts of the Community for Software Assurance-related standardization
ISO/IEC JTC1

- **SC22:** ISO/IEC Technical Report (TR) 24772 Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use.
  - This technical report was reviewed and approved by the project editor, then published in October 2010.
  - As published, the document includes language-independent summaries of nearly 70 classes of vulnerabilities.
  - The working group is already drafting the 2\textsuperscript{nd} Edition of the report which will add information specific to individual programming languages.

- **SC7:** ISO/IEC 15026, System and Software Assurance
  - Publication of the standard, by both ISO/IEC and IEEE, in spring 2011.
System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycle.

Terms of Reference changed: ISO/IEC JTC1/SC7 WG7, previously “System and Software Integrity” SC7 WG9.
ISO/IEC/IEEE 15026 Assurance Case

- Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources

Sub-parts
- A high level summary
- Justification that product or service is acceptably safe, secure, or dependable
- Rationale for claiming a specified level of safety and security
- Conformance with relevant standards & regulatory requirements
- The configuration baseline
- Identified hazards and threats and residual risk of each hazard / threat
- Operational & support assumptions

Attributes
- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages
Common Criteria v4 CCDB

- TOE to leverage CAPEC & CWE
- Also investigating how to leverage ISO/IEC 15026 NIAP Evaluation Scheme
- Above plus
- Also investigating how to leverage Security Content Automation Protocol (SCAP)
Many DHS & DoD sponsored efforts are key to changing how software-based systems are developed, deployed and operated securely.
Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related software system process, people and documentation.

**Process, People & Documentation**
- Evaluation Environment
  - Some point tools to assist evaluators but mainly manual work
  - Claims in Formal SBVR vocabulary
  - Evidence in Formal SBVR vocabulary
  - Large scope requires large effort

**Software System / Architecture Evaluation**
- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

**Claims, Arguments and Evidence Repository**
- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Reports
Risk Analysis, etc)

Protection Profiles
CWE
CWRAF/CWSS Provides Risk Prioritization for CWE throughout Software Life Cycle

• Enables education and training to provide specific practices for eliminating on software fault patterns;

• Enables developers to mitigate top risks attributable to exploitable software;

• Enables testing organizations to use suite of test tools & methods (with CWE Coverage Claims Representation) that cover applicable concerns;

• Enables users and operation organizations to deploy and use software that is more resilient and secure;

• Enables procurement organizations to specify software security expectations through acquisition of software and services.
Need for Rating Schemes

Rating of Suppliers providing software products and services
- Standards-based or model-based frameworks to support process improvement and enable benchmarking of organizational capabilities
- Credential programs for professionals involved in software lifecycle activities and decisions

Rating of Software products:
- Supported by automation
- Standards-based
- Rules for aggregation and scaling
- Verifiable by independent third parties
- Labeling to support various needs (e.g., security, dependability, etc)
- Meaningful and economical for consumers and suppliers

Collaborate with OWASP “Security Facts” labeling efforts
IT/Software Supply Chain Management is a National Security & Economic Issue

► Adversaries can gain “intimate access” to target systems, especially in a global supply chain that offers limited transparency

► Advances in science and technology will always outpace the ability of government and industry to react with new policies and standards
  - National security policies must conform with international laws and agreements while preserving a nation’s rights and freedoms, and protecting a nation’s self interests and economic goals
  - Forward-looking policies can adapt to the new world of global supply chains
  - International standards must mature to better address supply chain risk management, IT security, systems & software assurance
  - Assurance Rating Schemes for software products and organizations are needed

► IT/software suppliers and buyers can take more deliberate actions to security-enhance their processes and practices to mitigate risks
  - Government & Industry have significant leadership roles in solving this
  - Individuals can influence the way their organizations adopt security practices

Globalization will not be reversed; this is how we conduct business — To remain relevant, standards and capability benchmarking measures must address “assurance” mechanisms needed to manage IT/Software Supply Chain risks.
SOFTWARE ASSURANCE FORUM

“Building Security In”
https://buildsecurityin.us-cert.gov/swa
Cyber Infrastructure represents the convergence of information technology and communications systems, is inherent to nearly every aspect of modern life.

Illustrative examples only -- not all inclusive.