

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Software Assurance Contributions for a Secure Cyber Future

March 2012



Homeland
Security

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division



SOFTWARE ASSURANCE FORUM

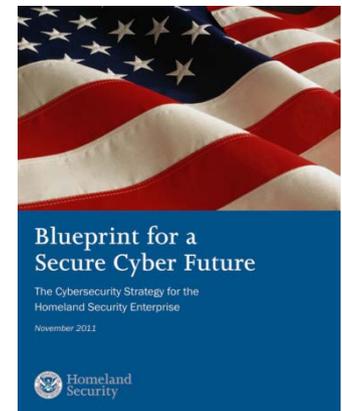
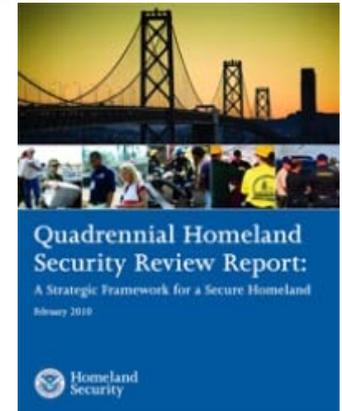
BUILDING SECURITY IN

Guidance

The 2010 Quadrennial Homeland Security Review (QHSR)¹ established a strategic framework to guide the activities of the homeland security enterprise toward a common end.

The Blueprint for a Secure Cyber Future (the Blueprint)² provides a clear plan of action for the homeland security enterprise to implement the National Security Strategy and achieve the goals set forth in the QHSR:

- To Create a Safe, Secure, and Resilient Cyber Environment, and
- To Promote Cybersecurity Knowledge and Innovation.



1. http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

2. <http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals of the Blueprint

Protect Critical Infrastructure:

- *Reduce Exposure to Cyber Risk*
- *Ensure Priority Response and Recovery*
- *Maintain Shared Situational Awareness*
- *Increase Resilience*

Strengthen the Cyber Ecosystem:

- *Empower Individuals and Organizations to Operate Securely*
- *Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures*
- *Build Collaborative Communities*
- *Establish Transparent Processes*

The Software Assurance Working Groups collaborate on providing capabilities.



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Protect Critical Infrastructure:

- ***Reduce Exposure to Cyber Risk***
- *Ensure Priority Response and Recovery*
- *Maintain Shared Situational Awareness*
- *Increase Resilience*



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Reduce Exposure to Cyber Risk

1. **Avert Threats:** *Decrease the ability of domestic and international criminals, including malicious insiders and foreign adversaries to exploit, impair, deny access to, or destroy critical information infrastructure, in part through the continued implementation of the Department's National Cybersecurity Protection System (NCPS).*

SwA Products / Capabilities Enabling Security Automation:

- CAPEC™
- CybOX™
- MAEC™
- OVAL™



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Reduce Exposure to Cyber Risk

- 2. Identify and Harden Critical Information Infrastructure:** Deploy appropriate security measures to manage risk to critical systems and assets.
- 3. Pursue Operational, Architectural, and Technical Innovations:** Develop new ways to address existing problems and research solutions to counter emerging security challenges.

SwA Products / Capabilities:

- DHS S&T BAA and SwAMP
- 
- 
- 
- 
- DHS Management Directives with SELC
- 
- SwA BSI and CRIC
- FISMA leveraging the use of CVE, OVAL, CWE, CAPEC, MAEC, CybOX
- TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Protect Critical Infrastructure:

- *Reduce Exposure to Cyber Risk*
- ***Ensure Priority Response and Recovery***
- *Maintain Shared Situational Awareness*
- *Increase Resilience*



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Ensure Priority Response and Recovery

- 4. Leverage the Enterprise in Taking Priority Actions:** *Unify efforts to collaboratively respond to and rapidly recover from significant cyber incidents that threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation.*
- 5. Prepare for Contingencies:** *Routinely conduct tabletop and functional exercises to test contingency plans and capture lessons learned.*

SwA Products / Capabilities:

- CAPEC
- MAEC
- CVE

- OVAL
- CWE
- CybOX

- TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Protect Critical Infrastructure:

- *Reduce Exposure to Cyber Risk*
- *Ensure Priority Response and Recovery*
- ***Maintain Shared Situational Awareness***
- *Increase Resilience*



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Maintain Shared Situational Awareness

6. **Fuse Information:** *Synthesize information developed through varied internal, local, national, and international sources.*
7. **Distribute Information Efficiently:** *Use multiple platforms to provide timely distribution of specific, actionable information.*
8. **Provide Specialized and Continuing Security Training to the Cyber Workforce:** *Collaborate to identify and deliver specialized cybersecurity training which improves workforce competency levels.*

SwA Products / Capabilities:

- TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)
- **CWE**
- SwA Curriculum Project
- **CWSS**
- **CWRAF**
- SwA BSI and CRIC
- SwA Related Standards and Models



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Protect Critical Infrastructure:

- *Reduce Exposure to Cyber Risk*
- *Ensure Priority Response and Recovery*
- *Maintain Shared Situational Awareness*
- ***Increase Resilience***



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Increase Resilience

9. Increase System Fault Tolerance: *Be prepared to maintain critical operations in a degraded environment.*

SwA Products / Capabilities:

- 
- 
- 
- *SwA Related Standards and Models*
- *TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Strengthen the Cyber Ecosystem:

- ***Empower Individuals and Organizations to Operate Securely***
- *Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures*
- *Build Collaborative Communities*
- *Establish Transparent Processes*



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Empower Individuals/Organizations to Operate Securely

10. Develop the Cyber Workforce in the Public and Private

Sectors: *Maintain a strong cadre of cybersecurity professionals to design, operate, and research cyber technologies, enabling success against current and future threats.*

11. Build a Base for Distributed Security: *Provide individuals with tools, tips, education, training, awareness, and other resources appropriate to their positions that enable them to implement existing cybersecurity features and configurations in protocols, products, and services.*

SwA Products / Capabilities:

- SwA Curriculum Project
- SwA BSI and CRIC
- SwA Pocket Guides
- 
- SwA Requirements in NICE
- 
- 
- 
- SwA Related Standards and Models
- SwA Forums and WG



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Strengthen the Cyber Ecosystem:

- *Empower Individuals and Organizations to Operate Securely*
- ***Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures***
- *Build Collaborative Communities*
- *Establish Transparent Processes*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Make/Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures

- 12. Reduce Vulnerabilities:** *Design, build, and operate information and communication technology to specifically reduce the occurrence of exploitable weaknesses. Enable technology to sense, react to, and communicate changes in its security or its surroundings in a way that preserves or enhances its security posture.*
- 13. Improve Usability:** *Design trusted technology that is easy to use, easy to administer, rapidly customizable, and performs as expected.*

SwA Products / Capabilities:

- **CAPEC**
- **CYBEX (X.1500)**
- **SwA Pocket Guides**
- **MAEC**
- **SATE**
- **SAMATE**
- **Software ID**
- **SwA Related Standards and Models**





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Strengthen the Cyber Ecosystem:

- *Empower Individuals and Organizations to Operate Securely*
- *Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures*
- ***Build Collaborative Communities***
- *Establish Transparent Processes*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Build Collaborative Communities

- 14. Appropriately Validate Identities in Cyberspace:** *Use risk-based decision making for authentication, raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions and communication.*
- 15. Increase Technical and Policy Interoperability Across Devices:** *On a device-to-device level, strengthen collaboration, create new intelligence, hasten learning, and improve situational awareness.*
- 16. Automate Security Processes:** *Employ automated mechanisms for acting collectively in near real-time to anticipate and prevent incidents, limit the spread of incidents across participating devices, and minimize consequences.*

SwA Products / Capabilities:

- SwA Pocket Guides
- SwA Related Standards and Models
- Software ID
- SwA BSI and CRIC
- 
- 
- 
- 



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Goals

Strengthen the Cyber Ecosystem:

- *Empower Individuals and Organizations to Operate Securely*
- *Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures*
- *Build Collaborative Communities*
- ***Establish Transparent Processes***



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Establish Transparent Processes

17. Publicize the Root Causes and Extent of Adverse Events in

Cyberspace: *Widely share information on security hazards, analogous to how information about wellness and disease is reported by public health officials. Verify the location of incidents in existing and future top level domains (e.g., dot gov, dot com, and dot edu) and understand the causes, extent, and impact.*

18. Deploy Security Measures Based on Proven Effectiveness:

Share information about the security efficacy of cyber protocols, products, services, configurations, architectures, supply chains, and organizational processes.

SwA Products / Capabilities:

-  CAPEC
-  CWE
-  CVE
-  CWRAF
-  MAEC
- SwA Pilots
- SwA BSI and CRIC



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Establish Transparent Processes

- 19. Focus on the Return on Investment:** *Assess the organizational impact of cybersecurity investments on operating costs, capital budgets, business agility, and liability expenditures for data breaches or failure to meet service agreements.*
- 20. Incentivize Performance:** *Establish, maintain, and improve upon a system of goals and measures for cybersecurity.*

SwA Products / Capabilities:

- TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)
- **CWE**
- **CWSS**
- **CWRAF**
- SwA Program

25 High Priority *Blueprint* Capabilities, Grouped by *Blueprint* Goals

8 <i>Blueprint</i> Goals	25 High Priority Capabilities – <i>Blueprint</i> for a Secure Cyber Future
Reduce Exposure to Cyber Risk	Intrusion Detection System (1.1)
	Heightened Domestic / International Law Enforcement (1.2)
	Information Distribution on CII Threats (1.3)
	Guidelines / Incentives for Incident Reporting (1.5)
	Risk Assessment and Prioritization (2.3)
	Internal Network Monitoring and Measurement (2.5)
	Standards-Based Automation (2.6)
Ensure Priority Response and Recovery	R&D Focused on Security Priorities (3.1)
	Mature / Exercised Cyber Incident Response and Recovery Plans (4.2)
Maintain Shared Situational Awareness	Cyber Threat Investigations and Forensics Analysis (4.4)
	National Cybersecurity Protection System (NCPS) (6.1)
	Rapid Information Correlation from Disparate Sources (6.2)
	Information Sharing with Trusted Partners (6.3)
Increase Resilience	Economic Incentives for Collaboration (7.5)
	Conformance to Established Resilience Standards and Guidelines (9.3)
Empower Individuals and Organizations to Operate Securely	Workforce Retention (10.3)
Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures	Cybersecurity Awareness Campaigns (11.1)
	Security Product Evaluation / Validation (12.4)
	Fundamental Research to Advance Technology / Standards (12.5)
	Commercial Innovation Enabling New Technology Design (12.6)
Build Collaborative Communities	Agile Acquisition Processes (12.7)
Establish Transparent Processes	Processes and Design that Evolve with Innovation (14.3)
	Information Distribution to HS Enterprise Stakeholders / Partners (17.2)
	Dissemination of Information about Efficacy of Cyber Protocols (18.1)
	Definition of Goals / Outcomes / Actions to Define Success (20.1)

25 High Priority *Blueprint* Capabilities, Grouped by *Blueprint* Goals

8 <i>Blueprint</i> Goals	25 High Priority Capabilities – <i>Blueprint</i> for a Secure Cyber Future	SwA Contributions
Reduce Exposure to Cyber Risk	Intrusion Detection System (1.1)	MAEC, CybOX
	Heightened Domestic / International Law Enforcement (1.2)	
	Information Distribution on CII Threats (1.3)	CAPEC, CybOX, MAEC
	Guidelines / Incentives for Incident Reporting (1.5)	CAPEC, MAEC
	Risk Assessment and Prioritization (2.3)	CVE, CWE, CWRAF, CWSS, OVAL
	Internal Network Monitoring and Measurement (2.5)	SwAMP, BAA, R&D (CWE, CybOX, CAPEC)
	Standards-Based Automation (2.6)	DHS Management Directives with SELC, FISMA leveraging CVE, OVAL, CWE, CAPEC, MAEC, CybOX
	R&D Focused on Security Priorities (3.1)	DHS S&T BAA and SwAMP, DHS Management Directives with SELC, TAXII (CybOX, CAPEC, MAEC, CEE, IODEF), SwA BSI and CRIC
Ensure Priority Response and Recovery	Mature / Exercised Cyber Incident Response and Recovery Plans (4.2)	TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)
	Cyber Threat Investigations and Forensics Analysis (4.4)	CAPEC, MAEC
Maintain Shared Situational Awareness	National Cybersecurity Protection System (NCPS) (6.1)	TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)
	Rapid Information Correlation from Disparate Sources (6.2)	TAXII (CybOX, CAPEC, MAEC, CEE, IODEF)
	Information Sharing with Trusted Partners (6.3)	CybOX
	Economic Incentives for Collaboration (7.5)	
Increase Resilience	Conformance to Established Resilience Standards and Guidelines (9.3)	SwA Related Standards and Models

25 High Priority *Blueprint* Capabilities, Grouped by *Blueprint* Goals

8 <i>Blueprint</i> Goals	25 High Priority Capabilities – <i>Blueprint</i> for a Secure Cyber Future	SwA Contributions
Empower Individuals and Organizations to Operate Securely	Workforce Retention (10.3)	SwA Requirements in NICE
	Cybersecurity Awareness Campaigns (11.1)	SwA BSI and CRIC, SwA Forums and WG
Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures	Security Product Evaluation / Validation (12.4)	SATE/SAMATE, CWE, CVE
	Fundamental Research to Advance Technology / Standards (12.5)	CYBEX (X.1500)
	Commercial Innovation Enabling New Technology Design (12.6)	CAPEC, MAEC
	Agile Acquisition Processes (12.7)	SwA Working Groups
Build Collaborative Communities	Processes and Design that Evolve with Innovation (14.3)	SwA Working Groups
Establish Transparent Processes	Information Distribution to HS Enterprise Stakeholders / Partners (17.2)	CVE, CWE, CWRAF, SwA BSI and CRIC
	Dissemination of Information about Efficacy of Cyber Protocols (18.1)	SwA Pilots, SwA BSI and CRIC
	Definition of Goals / Outcomes / Actions to Define Success (20.1)	SwA Program