SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Software Assurance "End State" Objectives…

…Enabling Software Supply Chain Transparency

Homeland Security

Software Assurance "End State" Objectives…

- **Government, in collaboration with industry/academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses.
  - Collaboratively advanced use of software security measurement & benchmarking schemes.
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the software supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers delivered quality products with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims.
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks.
  - Standards and qualified tools would be used to certify software by independent third parties.
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

…Enabling Software Supply Chain Transparency

What if…

1. The Federal Government supported a culture more demanding of assured products with requisite levels of integrity and security, and in collaboration with industry and academia, would have organizations structured and funded to bring forward more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities in products.
2. Components requiring high assurance would be scrutinized, ensuring personnel in several disciplines remain mindful of changing threats and remain focused on discovering exploitable vulnerabilities in software throughout the lifecycle.
3. Acquisition managers would have sufficient information on risks posed by the supply chain with appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software, and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.
4. Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.

SwA Working Group Goals and Objectives (1 of 3)

Goal	Outcome
1) Help advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses.	Operations should inform development and acquisition of diagnostic results indicating exploitable vulnerabilities in products currently used or planned to be used in mission/business critical systems.
2) Collaboratively advance use of software security measurement & benchmarking schemes.	Have organizations structured and funded to bring forward more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities in products.
3) Promote use of methodologies and tools that enable security to be part of normal business.	Acquisition managers would have sufficient information on risks posed by the supply chain (appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software), and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.

SwA Working Group Goals and Objectives (2 of 3)

Goal	Outcome
4) Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.
5) Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.	Components requiring high assurance would be scrutinized, ensuring personnel in several disciplines remain mindful of changing threats and remain focused on discovering exploitable vulnerabilities in software throughout the lifecycle.
6) Relevant standards would be used from which to base business practices & make claims.	Federal Government supported a culture more demanding of assured products with requisite levels of integrity and security.

SwA Working Group Goals and Objectives (3 of 3)

Goal	Outcome
7) Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks.	Acquisition managers would have sufficient information on risks posed by the supply chain with appraisal information on their suppliers’ process capabilities to determine risks posed by the suppliers’ products and services to the acquisition project and to the operations enabled by the software, and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.
8) Standards and qualified tools would be used to certify software by independent third parties.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.
9) IT/software workforce had requisite knowledge/skills for developing secure, quality products.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.

P&P Working Group Out brief

Collaboration With Other Efforts

- SAFECode
- Rugged Software
- SEI
- NDIA Systems Engineering
- NDIA Cyber Division
- OWASP
- Open Group – OTTF
- QAI/QAAM
- ISO/IEC
- IEEE

Work Product Efforts

- Analyze recent surveys and determine trends and disconnects in current practices and adoption (In support of Goal 2)
- Communicate practices in the context of multiple stakeholders map current practices (from SAFECode, Microsoft, etc) and Requirements (NIST 800-53, NIST IR 7622, Regulations to the Assurance PRM and SwA Checklist (In support of Goal 4, 6, &8)
- Communication through industry events and Pocket Guides (In support of goal 9)

A&O Working Group Out brief

Collaboration With Other Efforts

Work Product Efforts

- Explore and define User requirements for cloud. Pilot concept by focusing on a requirements for a particular cloud service and incorporation of resilient and rugged requirements (In support of goal 5)
- Provide simplified (in English) guidance to acquisition that incorporates SMART measurement information into development (project and supplier level) and acquisition decision making (In support of goal 3)
- Communication through industry events and Pocket Guides (In support of goal 9)

Back up

SwA Working Group Goal Alignment (1 of 6)

Goal	Outcome	Work Product Objectives	WG
1) Help advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses.	Operations should inform development and acquisition of diagnostic results indicating exploitable vulnerabilities in products currently used or planned to be used in mission/business critical systems.	Understanding attack surface, reducing the attack surface, quantifying the reduction in development and operations for decisions in acquisition and sustainment. • Research the use of APT and data breach information to inform development threat modeling, attack surface, testing and acquisition decisions.	• TT&PE primary • Supported by collaboration with other WGs
2) Collaboratively advance use of software security measurement & benchmarking schemes.	Have organizations structured and funded to bring forward more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities in products.	Integration of risks stemming from exploitable vulnerabilities into organizational structure and funding. • Research surveys to identify trends (i.e. the Forester and Deloitte survey).	• P&P Primary • Supported by collaboration with other WGs

SwA Working Group Goal Alignment *(2 of 6)*

Goal	Outcome	Work Product Objectives	WG
3) Promote use of methodologies and tools that enable security to be part of normal business.	Acquisition managers would have sufficient information on risks posed by the supply chain (appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software), and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.	Knowledge of best practices for secure development in a digestible format for acquisition decisions. • Provide simplified (in English) guidance to acquisition that incorporates smart measurement information into acquisition decision making.	• A&O Primary • Supported by collaboration with other WGs

SwA Working Group Goal Alignment (3 of 6)

Goal	Outcome	Work Product Objectives	WG
4) Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.	Codified standards (i.e. ISO, TOG, OMG, ITU, NDIA, IEEE, OWASP, OPEN Group Making Security Measurable, Assurance for CMMI, etc). • Identify and collaborate with existing groups and provide input/influence based on foundational WG documents and lessons learned.	• P&P and TT&PE • Supported by collaboration with other WGs

SwA Working Group Goal Alignment (4 of 6)

Goal	Outcome	Work Product Objectives	WG
5) Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.	Components requiring high assurance would be scrutinized, ensuring personnel in several disciplines remain mindful of changing threats and remain focused on discovering exploitable vulnerabilities in software throughout the lifecycle.	Development and acquisition practitioners understand and leverage knowledge from operations and appropriately apply knowledge and quantifiable data to ensure risks to mission/business critical systems are minimized.	• P&P and A&O • Supported by collaboration with other WGs
6) Relevant standards would be used from which to base business practices & make claims.	Federal Government supported a culture more demanding of assured products with requisite levels of integrity and security.	Communicate expected practices in the context of government requirements (NIST SP 800-53 ; NIST IR 7622; Common Criteria, agency specific).	• P&P and A&O • Supported by collaboration with other WGs

SwA Working Group Goal Alignment (5 of 6)

Goal	Outcome	Work Product Objectives	WG
7) Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks.	Acquisition managers would have sufficient information on risks posed by the supply chain with appraisal information on their suppliers' process capabilities to determine risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software, and program managers would use that information as part of the trade-space in their acquisition risk mitigation efforts.	Best practices techniques and SDLC practices are supported by real world examples that demonstrate the value of their use.	• P&P • Supported by collaboration with other WGs

SwA Working Group Goal Alignment (6 of 6)

Goal	Outcome	Work Product Objectives	WG
8) Standards and qualified tools would be used to certify software by independent third parties.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.	Influence industry efforts and NIST guidance.	Achieved through Goals 2 and 6
9) IT/software workforce had requisite knowledge/skills for developing secure, quality products.	Suppliers would have assurance standards from which to base their business practices, and would begin to develop software to meet those standards and be able to make assurance claims about the safety, security and dependability of their software in order to increase sales in both the public and private sectors where demand for high assurance products is growing rapidly.	Training, and education programs to expand the workforce of capable practitioners and leadership that demands application of the knowledge during development, acquisition and integration of software components. (Curriculum development and adoption) Outreach and Resources on increase awareness of stakeholders (Conferences and Products)	• WET • Supported by collaboration with other WGs Achieved through products from Goals 1-8