June Working Group Accomplishments and Outputs Planned for September

Description	Why It Is Important	Status	Follow-up Planned
DHS/MITRE released version 1.0 of the Malware Attribute Enumeration and Characterization (MAEC)	MAEC is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns.	SwA Program sponsored the development and community collaboration leading to the release.	The MAEC Team is developing a capability to generate sample MAEC descriptions from dynamic analysis tool output. The MAEC Team set up a "MAEC Development Group" on Handshake, MITRE's social networking platform, to permit members of the MAEC Working Group to more easily participate and contribute content to the effort.
Pocket Guide (PG) on Workforce Education.	This PG is a collaborative resource for educators for their awareness, not a detailed curriculum.	Robin Gandhi presented the PG to the Workforce Education and Training (WET) Working Group (WG). Many thanks to Dr. Gandhi.	Recommend separating the training costs/duration from the certifications. Take a look at National Science Foundation Pocket Guide. Solicit comments from the SwA Community.
Software Assurance Automation Protocol (SwAAP)	SwAAP is the broad integration of a suite of automation initiatives to achieve software assurance. Security Content Automation Protocol (SCAP) is the government's use case of the larger SwAAP for buying tools that are SCAP compliant.	Currently, there is no SwAAP automation protocol for threat analysis or incident management. SCAP is just now maturing. Common Weakness Enumeration (CWE) is at Version 1.9. Common Attack Pattern Enumeration and Classification (CAPEC) is at Version 1.5. MAEC is at Version 1.0. Steve Christey is enhancing the Common Weakness Scoring System (CWSS). Paul Black is working on the Assurance "Food Label."	SwAAP will take about 5 or 6 years of development and we need to understand that. We need to know the Assurance Case: who and what was involved in the assuring of the system. We need to build use cases for repeatable processes against these enumerations.

Description	Why It Is Important	Status	Follow-up Planned
National Institute of Standards and Technology Interagency Report (NISTIR) #7622: Supply Chain Risk Management Practices for Federal Information Systems	Draft NISTIR 7622, *Piloting Supply Chain Risk Management Practices for Federal Information Systems*, is intended to provide a wide array of practices for Federal Agencies that when implemented will help mitigate supply chain risk. This is the first step in a much larger initiative, known as Comprehensive National Cybersecurity Initiative (CNCI) 11, of developing a comprehensive approach to managing supply chain risks.	Rama Moorthy presented this NISTIR. NIST released the draft publicly on Monday, June 26.	Invite Marianne Swanson to present presentation on the NISTIR 7622 and the next steps at the September/October Forum.
National Initiative for Cybersecurity Education (NICE)	The National Initiative for Cybersecurity Education (NICE) is an ongoing program to teach Americans sound cybersecurity practices. The program's goal is to enhance the security of the country, and it also will improve computer security in the workplace and at home, as well as prepare future employees in the cyber security workforce.	NICE evolved from the Comprehensive National Cybersecurity Initiative as its scope expanded from a federal government focus to a national one.	Communicate SwA Workforce Education and Training (WET) Working Group (WG) resources available for NICE use.

Description	Why It Is Important	Status	Follow-up Planned
CWE, CAPEC, MAEC, and CWSS updated	These improve the measurability of security through enumerating baseline security data, providing standardized languages as a means for accurately communicating the information, and encouraging the sharing of the information with users by developing repositories.	A total of 108 new CVE Identifiers were added to the public CVE List. Release of Draft 2 of Open Vulnerability and Assessment Language (OVAL) Version 5.8. Posted CWE Version 1.9.	The use cases for multiple tools and operational environments. July 28-29 – The CVE/OVAL/CWE/CAPEC Teams are scheduled to participate in a Making Security Measurable booth at "Black Hat Briefings 2010" in Las Vegas, NV. August 15-20 – The MITRE Team is scheduled to present a CWE/CAPEC/MAEC briefing at *6th Annual GFIRST National Conference* in San Antonio, TX. July 15-16 – The CAPEC Team is scheduled to participate in the Malware TEM hosted at MIT Lincoln Labs. The MAEC Team has completed version 1.0 of the MAEC schema, which focuses on the low-level attributes. July 14-15 – The MAEC Team will present a briefing about MAEC at the *2010 Malware and Bot Technology Reverse Engineering Technical Exchange Meeting* in Lexington, MA.

Description	Why It Is Important	Status	Follow-up Planned
NIST's Vision for Software Assurance (SwA)	NIST has adopted a three-tiered risk management approach that incorporates Organization and Governance, Mission and Business Process, and Information Systems and the environment of operations. NIST's 2010 focus areas and initiatives included systems and security engineering and application security guidance.	Nadya Bartol offered the many resources of this Community. Ross replied that is a great offer and he looks forward to the mechanics for making it happen.	SwA reaches out to Ron Ross to introduce SwA WG products and guidance that can benefit NIST special publications and FIPS standards.
The Federal Enterprise Architecture (FEA)	FEA is a key to cyber security as we architect our systems. We need to do a better job of ensuring our SwA requirements are articulated in the enterprise architecture.	New action suggested by Ron Ross of NIST	TBD
Pocket Guide "Understanding Product Characteristics Throughout the SDLC" identifies the most effective software assurance tools for each stage of the SDLCs.	To understand where automated tools can be best leveraged to support the implementation of software assurance activities and provide insight into the SwA-related product characteristics throughout the SDLC.	The document outline was presented and next steps for completion were discussed.	Continue to populate the content in preparation for review. Explore how the use of automated tools to understand and produce characteristics during the SDLC can contribute to NIST's three-tiered Enterprise Risk Management Framework.

Description	Why It Is Important	Status	Follow-up Planned
Understanding SwA Practice Implementation (A Self-Assessment Approach)	Organizations need to be able to quantify and baseline assurance and risk management activities to ensure rugged software and software services are being developed and acquired. Supply chain partners must achieve increased awareness and communication to effectively understand risk throughout the software supply chain.	Used the Assurance Process Reference Model as the foundation. Created draft mappings to Resiliency Management Model (RMM), Open Software Assurance Maturity Model (OSAMM), Build Security In Maturity Model (BSIMM), and Capability Maturity Model Integration (CMMI).	Validate the existing mappings and add mappings to additional resources. Leverage content of industry resources to incorporate developer and acquisitions considerations.
Developing Phase 2 for FSTC SwA Initiative	FSTC Phase 1 included research into literature and presentations by leaders in various related fields from representatives of the academic and vendor communities. The Phase 1 report identified a number of areas where contributions from the SwA Community are needed.	Laid the foundation for a collaborative path forward.	Collaborate with the FSTC/FS ISAC to define a path forward. Brief the path forward to the FS ISAC.
The SEI Virtual Training Environment (VTE)	The VTE presents our SwA training in a dynamic online format that is available on demand.	ACT online has been moved from Memphis to Texas A&M.	The WG is exploring ACM, AIS, and other curriculum building groups. Educators who are interested in teaching this curriculum are to contact the WET WG co-chairs.

Description	Why It Is Important	Status	Follow-up Planned
Master of Software Assurance Reference Curriculum.	Sponsored by NCSD SwA, this project provides materials for undergraduate and master's courses in software assurance on the "Build Security In" (BSI) website.	The Software Assurance Curriculum Team posted the draft materials for public review and comment with review forms. Presentation/ workshop materials are at https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html to promote faculty awareness or provide an overview of the curriculum work. These materials can be tailored to the presenter and the audience. They have already been used to support several presentations and workshops.	Explore the possibility of putting together a starter certificate, leading to a plan to analyze how to translate this to a graduate-level degree. Solicit comments from the SwA community. Completed review forms are requested by July 15 to bsi-curriculumreview@sei.cmu.edu
Software Assurance Mobile Instruction (SAMI)	SAMI is an iPod- and iPad-based curriculum application that will be given away to teachers at community colleges to educate their students.	SAMI is set up for distance learning. There are a myriad of resources already loaded onto the system. The WG needs to determine what constitutes success.	The WET WG will determine who the audience is and then market to this audience. The WG plans to determine what students need to learn from an industry perspective and what the software companies are teaching their employees. Potential conferences to present at include ANSYS and Institute of Electric and Electronic Engineers (IEEE). The WG plans to communicate its message outside the software industry. The message will include topics such as the top 10 items that industry would like students to know. The challenge to address is encouraging the students to want to make secure code.

Description	Why It Is Important	Status	Follow-up Planned
Develop an online collaboration tool and document repository with change control results.	Rapid collaboration is difficult via email exchange.	Wiki solutions are being investigated.	The WET WG is going to stand up a wiki to contribute to without an admin.