



# Software Assurance (SwA) Forum and Working Group Sessions Fact Sheet

## BACKGROUND

The Software Assurance (SwA) stakeholder community serves an essential role in protecting government applications, systems, and information from persistent and evolving threats. The SwA Forum and Working Group Sessions bring experts with various backgrounds and shared interests in software assurance to discuss and promote integrity, security, and resilience in software. Speakers and panels present updates on relevant programs and initiatives, practical solutions to mitigate security risks attributable to exploitable software, and research on technical solutions for both software process and product assurance.

Four times per year, under the co-sponsorship of organizations in the U.S. Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute for Standards and Technology (NIST), the SwA Forum and Working Group Sessions provide a venue for participants to share their knowledge and expertise in software security while interacting and networking with key leaders in industry, government, and academia. The gatherings are unique in focus by bringing together a stakeholder community to protect the Nation's key information technologies, most of which are enabled and controlled by software. The SwA Forum and Working Group Sessions are means for fulfilling the Open Government Initiative, reflecting the three principles of transparency, participation, and collaboration.

Multiple panels convey numerous viewpoints of the community and form the basis for SwA Working Group initiatives and goals to be further refined in follow-on meetings held after each Forum. Previous topics have included supply chain risk management; open source software security; cybersecurity roadmap for SwA community collaboration; and software assurance maturity models.

Recognizing that securing software is a shared responsibility, the SwA Forum and Working Group Sessions provide opportunities for participants to define short- and long-term objectives of the community collaboration efforts for the coming years and develop the shared strategic plan for meeting the objectives. The SwA stakeholder community identifies and revises these goals to respond to the changing cyber environment.

## BENEFITS

The benefits of participating in the SwA Forum and Working Group Sessions include the following:

- Make more informed decisions for mitigating risks attributable to software by learning about the latest advancements in software security trends and technologies.
- Establish better information-sharing relationships with federal partners, industry, academia, and international partners by collaborating with stakeholders in an open and transparent manner on advancing software assurance objectives.
- Gain greater situational awareness across multiple domains by drawing from a larger pool of expertise available at SwA Forums and Working Group Sessions.
- Qualify for Continuing Professional Education (CPE) credits from International Information Systems Security Certification Consortium, Inc. (ISC)<sup>2</sup> and Information Systems Audit and Control Association (ISACA).

## INTENDED OUTCOMES

SwA Forums and Working Group Sessions intend to accomplish the following outcomes:

- Promote integrity, security, and resilience in software.
- Increase awareness and implementation of SwA resources, tools, and solutions.
- Provide input to SwA education and training curricula.
- Inform acquirers about considerations and risks in the software supply chain.
- Develop an overarching approach to measure and interpret SwA information.
- Advance the awareness and understanding of and the demand for assured software.
- Develop a consensus on cataloging software common weaknesses and attributes.



# Software Assurance (SwA) Forum and Working Group Sessions Frequently Asked Questions (FAQs)

## **What is Software Assurance (SwA)?**

SwA is the level of confidence that software is free of vulnerabilities, either intentionally or unintentionally designed or inserted during software development and/or the entire software life cycle, and that the software functions in the intended manner (from CNSS 4009 IA Glossary - see [Wikipedia](#) for definitions and descriptions).

## **Why were the Software Assurance (SwA) Forum and Working Group Sessions created?**

Since creating the National Cyber Security Division (NCSD) in 2003, the Department of Homeland Security's (DHS) leadership recognized the need for public/private collaboration among software and cybersecurity professionals. Concurrently, the Department of Defense (DoD) stood up its Software Assurance Initiative and sought collaboration with other federal agencies. The result was the creation of the Software Assurance (SwA) Forum and Working Groups, co-sponsored by DHS NCSD, the DoD Office of the Secretary of Defense, and the National Institute for Standards and Technology (NIST). The SwA Forum and Working Group Sessions are part of the Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides the framework for participation.

## **What is the difference between the SwA Forum and the SwA Working Group Sessions?**

The format of the SwA Forum is similar to that of a conference in which subject matter experts deliver presentations followed by audience Q&A. The Forum is the best way for those new to SwA to obtain the background needed to participate in the Working Group Sessions. Although the Working Group Sessions may include keynote speeches and presentations regarding status updates, the Working Groups drive SwA initiatives forward by providing venues for public/private collaboration in advancing SwA and developing deliverables. Forums are scheduled in the spring and fall, while Working Group Sessions are held in the summer and winter.

## **When and where is the next SwA Forum or SwA Working Group session being held?**

The schedule for the upcoming SwA events, and presentations from past SwA Forums, are located on the [Build Security In website](#). <https://buildsecurityin.us-cert.gov>. To receive notices of upcoming SwA Forum or Working Group Sessions, send a request to: [software.assurance@dhs.gov](mailto:software.assurance@dhs.gov) To register for an upcoming event, send a request to: [softwareassurance@asballiance.com](mailto:softwareassurance@asballiance.com).

## **Do I have to be a member of a group to attend the SwA Forum and Working Group Sessions?**

No, the SwA Forum and Working Group Sessions are free and open the public.

## **Is there a fee to attend the SwA Forum and/or Working Group Sessions?**

No, there is no fee to attend any SwA Forum or SwA Working Group Sessions. However, pre-registration is required. Expenses associated with travel, lodging, and meals are the responsibility of those attending.

## **Who attends the SwA Forum or Working Group Sessions?**

Participants represent a diverse group of career professionals including government officials, chief information security officers, those in academia with cybersecurity specialties, system administrators, engineers, consultants, vendors, software developers, managers, analysts, specialists in IT and cybersecurity, and many more fields.

## **Where can I obtain more information about software security?**

Additional information and resources in software assurance and cybersecurity are available online:

- SwA Build Security In (BSI): <https://buildsecurityin.us-cert.gov>
- SwA Community of Resources & Information Clearinghouse: <https://buildsecurityin.us-cert.gov/swa/>
- Software Assurance Metrics and Tool Evaluation (SAMATE): <http://samate.nist.gov>
- Software Security Automation & Making Security Measureable: <http://measurablesecurity.mitre.org/>