Welcome to the MULTI-CLOUD SECURITY PUBLIC WORKING GROUP (MCSPWG)

FALL 2022

National Institute of Standards and Technology
U.S. Department of Commerce

The meeting will begin shortly!

mcsec@nist.gov

MCSPWG – General Purpose

- Aligned with NIST's mission:

  - ✓ *Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.*
  - ✓ *NIST works to maximize its impact and mission fulfillment by positioning itself to anticipate future technology trends and develop the most important measurements and standards products that are aligned with industry drivers and needs.*

- Build a community of experts on cloud security interested in complex multi-cloud architectures (bring new members and encourage existing members to get involved)
- Research, identify and document multi-cloud adoption challenges
- Research, propose and document best practices for addressing the identified challenges

AC-21 ✓

AUTOMATION

NIST

Search CSRC | ☰ CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Multi-Cloud Security Public Working Group MCSPWG

Overview

Cloud computing has become the core accelerator of US Government digital business transformation. NIST is establishing a Multi-Cloud Security Public Working Group (MCSPWG) to research best practices for securing complex cloud solutions involving multiple service providers and multiple clouds.

The White House Executive Order on *Improving the Nation's Cybersecurity* highlights that "*the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life*" by focusing "*the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid*." The MCSPWG research will focus on a) identifying the challenges of implementing secure multi-cloud systems and b) developing guidance and best practice for mitigating the identified challenges.

The US federal agencies were further encouraged by the Cloud Smart Federal Computing Strategy to accelerate cloud adoption and modernize their IT infrastructures, leverage cloud technology scalability and speed-to-market by expanding and diversifying their cloud portfolio to incorporate multi-party (multi-providers) cloud solutions. Many organizations in adopting these cloud solutions, which can include services provided by different cloud service providers often with support from third-party entities, are faced with added security and privacy implementation challenges.

The MCSPWG Charter provides additional information on MCSPWG including the planned work and the rules of engagement for participation and subscription to the mailing list below.

Leadership

Credits: Annie Sokol

ANNIE SOKOL

IT Specialist

NIST

ITL/CSD/SSA

Credits: Brian Ruf

BRIAN RUF

Director of Cybersecurity

Easy Dynamics

Credits: Austen Bryan

Austen Bryan

ex-COO, DoD Platform One

Delivery Manager

Defense Unicorns

Credits: Ned Goren

NED GOREN

IT Specialist

NIST

ITL/CSD/SERM

PROJECT LINKS

Overview

Presentations

ADDITIONAL PAGES

Charter

Leadership

Meetings

Related References

GROUP

Secure Systems and Applications

TOPICS

Security and Privacy: access authorization, access control, authentication, general security & privacy, privacy engineering, risk assessment, system authorization, systems security engineering, threats

Technologies: cloud & virtualization

RELATED PROJECTS

Cloud Computing

Cloud Forensics

Disclaimer

Certain commercial multi-cloud solutions (or providers) might be mentioned, discussed or discussed as part of this research.

Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the services identified are necessarily the best available for the purpose.

Ground Rules of Engagement

- Keep the discussion respectful by:
  - using welcoming and inclusive language
  - being respectful of differing viewpoints and experiences
  - gracefully accepting constructive criticism
  - wait for one speaker to finish before speaking
- Speak from your own experience instead of generalizing.
- Do not be afraid to respectfully challenge one another by asking questions focused on ideas not on the company or presenter.
- The goal is not to always agree but rather gain a deeper understanding.

Today's Agenda

1. **Introduction of the new co-chairs**
   https://csrc.nist.gov/Projects/mcspwg/leadership
2. **Review of the Concept of Operations (ConOps) and Research Strategy**
   Google Drive:
   https://drive.google.com/drive/folders/1c9OV10sAQGFRMplsQALSrKNMtjqKx1CQ?usp=sharing
3. **Open floor**

Thank you for joining us!

NEXT MCSPWG MEETING: SEPTEMBER 26, 2022

https://csrc.nist.gov/Projects/mcspwg/meetings

NIST | mcsec@nist.gov
mailing list: mcspwg@list.nist.gov