# HotSoS 2026 Call for Papers

13th Annual **HOT TOPICS** in the **SCIENCE OF SECURITY (HoTSoS)** hotsos.org
April 14-16 2026 | ***virtually*** hosted by **THE NATIONAL SECURITY AGENCY**

**Hot Topics in the Science of Security (HotSoS)** is a forum for presenting and discussing the latest research and development advances in the scientific foundations of cyber security and privacy. In the pursuit of mentorship and advancement of knowledge, the forum brings together researchers, practitioners, and thought leaders from government, industry, and academia. The National Security Agency (NSA) sponsorship of HotSoS provides for a collaborative relationship with NSA researchers, practitioners, and leaders and results in a unique attendee audience. The HotSoS vision is to engage and grow a community that includes researchers and skilled practitioners from diverse disciplines focused on the advancement of scientific methods. The event provides networking and mentoring opportunities to advance the scientific research careers of students. HotSoS`26 will continue to pioneer new methods to have impactful virtual events in April 2026. In addition to research paper discussions and presentations, the symposium program will also include invited talks, panels, and posters. We solicit submissions in the following three categories:

1. **Published Research papers** will be accepted for presentation, provided their scope aligns with HotSoS.
2. **Works-in-Progress papers (WiP)** will be evaluated for scope, potential for impact, and technical merit. Papers in this category will be discussed during the special WiP session and receive detailed feedback towards making the paper publishable at a top-tier venue. We are looking for bold, risky, and interdisciplinary ideas.
3. **Poster/Demo abstracts** will be selected for brief presentations and highlighted by a poster/demo competition.

## SUBMISSION REQUIREMENTS

All papers and manuscripts should be submitted via Open Review: https://openreview.net/group?id=HotSoS.org/2026/Symposium#tab-your-consoles

**Already Published Research Papers**
When submitting, specify the submission category to be **"already published research papers"**. Submissions may use the format of the published venue.

**Works-in-Progress Papers**
When submitting, specify the submission category to be **"Works-in-Progress papers."** WiP papers should be at most 10 pages in the double-column ACM format including the bibliography or, alternatively, 9 pages not including the bibliography. Note that WiP papers are encouraged even if they are substantially shorter than the page limit. The paper may have optional appendices, but reviewers are not required to read them. Submissions must be in PDF format and the title should begin with "WiP: ."

Each author must assert that the manuscript is unpublished and revisions can be incorporated into the manuscript prior to their next submission for publication. Prior publication includes the appearance in a proceeding, online or in print, of any version of the work that received peer review, including short papers. Posters and online, pre-submission non-archival versions of non-peer reviewed papers will not be considered prior publication. Pre-submission non-archives include arXive.org and CiteSeerX. A short paper version of a submission may not immediately disqualify the submission, however, and the committee will consider the differences in the versions prior to making final decisions. Thus, authors are encouraged to briefly disclose in a cover page to their submission any prior submissions and/or publications related to the submission ACM Template: https://www.overleaf.com/gallery/tagged/acm-official#.WlayAkt-G3v0

**Poster/Demo Submissions**
When submitting, specify the submission category to be **"poster or demo presentation."** Accepted posters/demos will be displayed on the symposium website. Each extended abstract should be at most 2 pages, including citations and references. Both abstracts and draft poster files are accepted.

**Government and Industry Talks**
Nominations or proposals for government or industry talks can be sent directly to the program chairs via email at hotsos2026@sos-vo.org.

## TOPICS OF INTEREST

HotSoS is seeking high-quality submissions of foundational cybersecurity research. Submissions that overlap with any of the following areas are encouraged:

**Defense of AI/ML Systems to Adversarial Behavior**
- Multi-turn and long-context jailbreaks and defenses in interactive systems
- Approaches for durable safety alignment
- Security threats in multi-modal and cross-modal large models
- Mechanistic analyses of LLMs with implications for safety and reliability
- Systematic red teaming methodologies
- Adversarial dynamics in multi-agent and agentic AI systems
- Adversarial attacks and defenses on reasoning, and planning capabilities
- Data poisoning, backdoors, and training-time vulnerabilities

**Applications of AI/ML to Cybersecurity Challenges**
- Analyses of LLMs in cybersecurity
- Novel Machine Learning architectures for cybersecurity
- Cybersecurity analyses of AI Algorithms and Systems
- Defenses against AI-enabled adversaries
- Agentic AI systems

**Computer & Network Security**
- Operating in degraded/compromised environments
- Static and dynamic analyses for securing software, reverse engineering, or other cybersecurity activities
- Scalable and composable frameworks for security
- Complex, distributed, and/or decentralized system security
- Design principles, tools, and architectures for provably secure systems and continuous monitoring and continuous authorization
- Security of cyber-physical, service mesh networks, embedded, and autonomous systems

**Other Security Topics**
- Systemization of Knowledge (SoK) and research methods
- Analytic Assessments of Cyber Risks
- Decisions Models for Cybersecurity
- Human subjects research relating to cybersecurity tools, practices and decision-making
- Ethical considerations in AI, security, and privacy
- Any other cybersecurity-related submissions are welcome aside from cryptography and offensive security

## IMPORTANT DATES

- **Submission Deadline: December 23, 2025**
- **Notification to Authors: February 27, 2026**
- **Virtual Symposium: April 14-16, 2026**

Please send any questions about topics or submission requirements to hotsos2026@sos-vo.org

## ORGANIZATION

**General Chair**
Adam Tagert (National Security Agency)

**Program Co-Chairs**
Jonathan Aldrich (Carnegie Mellon University)
Benjamin Erichson (ICSI Berkeley)