SUNS

# *Synopsis of the March 2023 Software Understanding for National Security (SUNS) Workshop*

**October 2023**

Web https://suns.sandia.gov/
Email suns@sandia.gov

The SUNS workshop was funded through an interagency agreement (70RSAT21KPM000105) with the Department of Homeland Security's Science and Technology Directorate.

## Overview

The Software Understanding for National Security (SUNS) Workshop was held March 6th-10th, 2023 at the Cybersecurity and Infrastructure Security Agency (CISA) in Arlington, VA. The purpose of the workshop was to gather experts and solicit their opinions on a range of issues to help illuminate possible paths forward for tackling the problem of software understanding in the U.S. government (USG). The workshop was hosted by the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate, with support from Sandia National Laboratories, a federally funded research and development center focused on tackling challenging problems in national security.

The workshop consisted of both technical and non-technical sessions. Experts with experience in building automated tools for the behavioral analysis of software discussed technical impediments, necessary stakeholder support, and vital research and development (R&D) gaps. Over the course of the workshop all participants heard a variety of presentations about the nature, need, and challenges that the nation faces given the ubiquity and proliferation of software across so many national security and critical infrastructure missions.

The SUNS Workshop focused on examining the underlying technical landscape to inform policy deliberations. The workshop prioritized focused technical discussions with subject matter experts during a three-day technical sprint during which the experts expressed their individual opinions on a wide range of critical issues. Open sessions were held on Monday and Friday. These discussions explored the challenges and possible paths forward for producing the software understanding technical capabilities required to meet national security and critical infrastructure mission needs.

This document presents a broad overview of the workshop, including: the attending organizations, the content of the session discussions, and a synopsis of the workshop's key results. In addition to this document, the SUNS organizers will also be releasing a SUNS 2023 Workshop Report that will dive into topics from the workshop, including SME straw poll results, non-technical impediments, and near-term research priorities.

## The Challenge

Our nation’s leaders rely on third-party software to fulfill the most important national commitments—the defense of the country, public trust and confidence in essential services and institutional competence, and a strong, growing, and vibrant economy. The proliferation and ubiquity of software across all major segments of the economy broadens this reliance. Despite rigorous testing, software may contain unexpected behavior, including bugs, weaknesses, vulnerabilities, or even hidden malicious functionality. These unexpected behaviors are challenging to identify, let alone manage, yet could imperil the USG missions that rely on such software. The inability to adequately analyze this software to answer vital mission questions creates unbounded risk for the USG.

This national challenge—expanding risk to our institutions, coupled with underdeveloped software analysis approaches that rely too heavily on unscalable manual analysis—will only worsen as national security and economic pressures drive the need for innovation based on digital technologies.

Congress and the Administration have taken serious steps to address these threats and gaps. However, while bold policy measures are necessary, alone they are fundamentally insufficient to address this challenge. Effective policy measures must rest on the strength of technical competencies. What is lacking—and what the workshop aimed to address—is a robust technical capability to analyze third-party software, deriving technical evidence from the software itself at the speed of mission to inform risk decisions.

## The SUNS 2023 Workshop

Five USG stakeholders convened a five-day gathering of select government researchers and mission stakeholders to discuss the technical aspects of this national need.  The Software Understanding for National Security (SUNS) Workshop prioritized focused discussions with technical experts designed to solicit their individual opinions on the underlying technical landscape of the capabilities needed to address the nation’s technical challenges in adequately understanding the software upon which the nation relies.

## SUNS Participants

The SUNS 2023 Workshop was convened by five government co-conveners and was attended by over 90 attendees from 19 organizations.

### Co-conveners

The SUNS 2023 workshop was convened by five government representatives, listed alphabetically:

- Christopher Butera
  Technical Director of Cybersecurity
  Cybersecurity and Infrastructure Security Agency (CISA)
- Edward Jakes
  Director, Nuclear Enterprise Assurance Division
  National Nuclear Safety Administration (NNSA)
- Dr. Garfield Jones
  Associate Chief of Strategic Technology
  Cybersecurity and Infrastructure Security Agency (CISA)
- Dr. Robert Runser
  Technical Director of Research
  National Security Agency (NSA)
- Neal Ziring
  Technical Director of Cybersecurity
  National Security Agency (NSA)

### Open Session

The open sessions consisted of over 90 attendees, representing the following organizations, listed alphabetically:

- Carnegie Mellon University, Software Engineering Institute (SEI)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Defense Advanced Research Projects Agency (DARPA)

- Defense Intelligence Agency (DIA)
- Department of Homeland Security, Science & Technology Directorate (DHS S&T)
- Department of the Army
- Georgia Tech Research Institute (GTRI)
- Institute for Defense Analyses, Center for Computing Sciences (IDA/CCS)
- Lawrence Livermore National Laboratory (LLNL)
- MIT Lincoln Laboratory (MIT-LL)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)
- Office of Naval Research (ONR)
- Office of the Director of National Intelligence (ODNI)
- Office of the National Cyber Director (ONCD)
- Office of the Secretary of Defense (OSD)
- Pacific Northwest National Laboratory (PNNL)
- Sandia National Laboratories (SNL)
- Zeichner Risk Analytics (ZRA)

## Closed Session

The 29 members of the closed technical session included experts in the field of software understanding from government research, Federally Funded Research Centers (FFRDCs), and University Affiliated Research Centers (UARCs). These technical SMEs represented the following organizations:

- Carnegie Mellon University, Software Engineering Institute (SEI)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Defense Advanced Research Projects Agency (DARPA)
- Georgia Tech Research Institute (GTRI)
- Institute for Defense Analyses, Center for Computing Sciences (IDA/CCS)
- Lawrence Livermore National Laboratory (LLNL)
- MIT Lincoln Laboratory (MIT-LL)
- National Security Agency (NSA)
- Pacific Northwest National Laboratory (PNNL)
- Sandia National Laboratories (SNL)

### Panelists

The open sessions included a panel discussion of the needs, risks, and challenges for a revolutionary approach to software understanding for third-party and legacy software in national security and critical infrastructure missions. The following individuals participated on the panel, listed alphabetically:

- Carlton Brooks
  Technical Director, Nuclear Command and Control Systems (NCCS)
  Cybersecurity, National Security Agency (NSA)
- Cherylene Caddy
  Deputy Assistant National Cyber Director
  Office of the National Cyber Director (ONCD)
- Dr. Ryan Craven
  Program Officer, Cyber S&T
  Office of Naval Research (ONR)
- Bob Lord
  Senior Technical Advisor
  Cybersecurity and Infrastructure Security Agency (CISA)

## Workshop Breakdown

The workshop sessions were split into an open component that took place on Monday and Friday and a more technically focused component which occurred Tuesday through Thursday.

The SUNS workshop began and ended with sessions of interest to a broader audience of mission stakeholders, program managers, and decision-makers. Monday's sessions included keynote presentations from the co-conveners present, presentations on case studies in software understanding, and a panel session. Collectively, Monday's sessions provided attendees an opportunity to broadly consider the software understanding needs across multiple mission areas and the nature of the technical challenges. In contrast, Friday's sessions focused on reporting the results from the technical discussions on Tuesday through Thursday.

The technical sprint on Tuesday, Wednesday, and Thursday gave the experts an opportunity to express their individual technical opinions on current capabilities, gaps, and possible future of automated software analysis tools. These sessions were restricted to select technical SMEs with at least 5 years of hands-on experience creating software analysis tools to understand third-party software, and experience applying such tools to one or more critical infrastructure or national security missions. Breakout session topics discussed during the technical sprint included: non-technical impediments, technical challenges common to today's software understanding tools, technical strategies to address multiple mission questions and programs under test, approaches to developing a robust software analysis ecosystem, and recommended near-term research and development priorities.

The SUNS 2023 Workshop Report will detail these discussions and provide an overview of expert opinions expressed by the SMEs in technical statements, during workshop discussions, and through informal "straw polls" that took place throughout the three days.

## Workshop Results Summary

By the end of the closed sessions, a majority (in some cases all) of the SMEs participating expressed opinions consistent with the following key results from the workshop:

First, on the question of the technical capability improvements in software understanding, a 10x-100x+ improvement in software understanding capabilities is possible, but lack of a centralized vision, funding that is 10x+ too low, inability to collaborate, and other non-technical issues currently prevent this progress.

Second, 14 near-term R&D ideas could be used to prioritize near-term investment decisions.

Third, there is strong desire to see a government-wide community of software understanding researchers established.  To this end, the SUNS 2023 Workshop was the first time many of these like-minded researchers had ever met and even contemplated establishing a government-wide community.

Fourth, to meet the nation's technical challenges in software understanding, collaboration among the technical community is essential.  Specifically, there is a compelling need to cultivate a strong community of researchers that can share, collaborate, communicate, and otherwise work effectively across government and government-affiliated organizations. Without such a strong community, revolutionary progress would be impossible. However, a straw poll of the SMEs taken during the workshop, showed the most widely held opinion to be that, if the only change that occurs is to enable the SUNS SME community to collaborate seamlessly, a 5-10x improvement in software understanding capabilities could be realized over the next 10 years. Additionally, a variety of factors currently hinder the formation of that community.

Finally, during Friday's closed session, the technical SMEs identified issues to "run up the flagpole" for special consideration by the co-conveners and the federal government. These "flagpole issues" were those the SMEs each felt were the most important impediments to address to make progress on a national software understanding capability. The top five flagpole issues identified by the SMEs were:

1. **Software Understanding Vision:** The community lacks a broadly agreed-upon vision and coordinated research agenda. As a result, this can hinder the impact and ability to answer mission questions. An entity should be responsible for generating and sustaining a vision statement as it could promote a research agenda with informed priorities and external engagements and investments.

2. **Community Building:** The community is fragmented and operates in highly siloed groups, allowing only marginal progress in software understanding capabilities. Consequently, there is a need to identify the existing community, grow the community, and collaborate to sustain the community.

3. **Sharing and Collaboration:** Tools and data in today's environment are not adequately shared. A culture of real collaboration on this issue does not

currently exist and even basic issues like sharing code repositories can be complex. As a result, this creates bottlenecks and can lead to siloed findings.

4. **Funding:** Existing funding options for research in these areas generally have too short a timeframe, do not support the necessary foundational research, and offer insufficient overall funding. Achieving the available advances in national capabilities requires dedicated and sustained funding for not only the foundational research but also the practical development and engineering of the ecosystem necessary for that research to thrive.

5. **Challenge Problems, Data Sets, and Benchmarks:** The community needs challenge problems, data sets, and benchmarks to drive and observe progress in software understanding.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2024-04945R