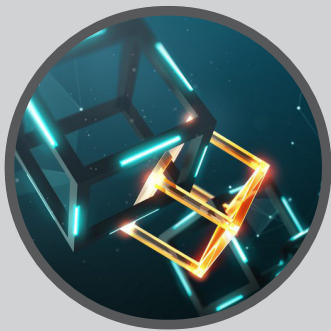


CYBERSECURITY & Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // January 9, 2024



STATE-OF-THE-ART REPORT (SOAR)

CSIAC is pleased to announce publication of our latest State-of-the Art Report (SOAR) on "Blockchain Applications for Federal Government," which reviews fundamentals of the technology, its applications, limitations, and more.

More information about the SOAR is available on our website at <https://csiac.org/state-of-the-art-reports/blockchain-applications-for-federal-government/>.

DID YOU MISS OUR LAST WEBINAR?

"Optimization Techniques: Improving Effectiveness for Defense..."

[WATCH NOW!](#)

[or download the slides](#)

NOTABLE TECHNICAL INQUIRY

Is there an overarching Wi-Fi program for the U.S. Air Force?

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) was tasked with researching and identifying an all-encompassing wireless technology program for wireless communications on flight lines used by the United States Air Force (USAF). CSIAC identified wireless... [READ MORE](#)

UPCOMING WEBINAR



Developing the Cybersecurity Workforce...

January 25, 2024
12:00 PM – 1:00 PM

Presenter(s): Karen Wetzel

Host: CSIAC

The Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education [NICE] Framework) (NIST SP 800-181r1) establishes a common language for describing cybersecurity work and what needs done to complete that work. It is used by government, academia, and private... [READ MORE](#)

FUTURE WEBINARS

The Art and Science of Metawar

February 7, 2024
12:00 PM – 1:00 PM

Uncomfortable Truths About Cybersecurity

March 13, 2024
12:00 PM – 1:00 PM



2023 NSA CYBERSECURITY

{ Year In Review

U.S. DoD

HIGHLIGHT

NSA Publishes 2023 Cybersecurity Year in Review

FORT MEADE, Md.--The National Security Agency (NSA) recently published its 2023 Cybersecurity Year in Review to share its cybersecurity successes and how it is working with partners to deliver on cybersecurity advances that enhance national security. This year's report highlights NSA's work with... [LEARN MORE](#)

EVENTS

Washington DC SASE Summit

January 24, 2024
Washington, DC

CyberSmart 2024

January 25, 2024
Reston, VA

Google Defense Forum

January 25, 2024
Pentagon City, VA

Automotive Cybersecurity, Connectivity & SDV

February 12-13, 2024
Virtual

Rocky Mountain Cyberspace Symposium (RMCS24)

February 19-22, 2024
Colorado Springs, CO

Advantage DoD 2024: Defense Data & AI Symposium

February 20-23, 2024
Washington, DC

Want your event listed here?

Email contact@csiac.org, to share your event.



VOICE FROM THE COMMUNITY

Timothy Ruppert

Certified Cyber Crime Investigator

Timothy Ruppert is a certified cyber crime investigator in the private sector, where he tracks, disrupts, and unmask malicious actors targeting cloud resources and infrastructure. He is a former analyst for multiple federal law enforcement agencies.

ARE YOU A SME?

If you are a contributing member of the information systems community and are willing to help others with your expertise, you are a subject matter expert (SME).

Join our team today!

**BECOME A SUBJECT
MATTER EXPERT**

ABOUT TECHNICAL INQUIRIES (TIs)

WHAT IS THE TI RESEARCH SERVICE?

- FREE service conducted by technical analysts
- 4 hours of information research
- Response in 10 business days or less

WHO CAN SUBMIT A TI?

- U.S. government (federal, state, or local)
- Military personnel
- Contractors working on a government or military contract

WHY UTILIZE THE TI RESEARCH SERVICE?

- Get a head start on your technical questions or studies
- Discover hard-to-find information
- Find and connect with other subject matter experts in the field
- Reduce redundancy of efforts across the government

To submit a TI, go to <https://csiac.org/technical-inquiries>

FOR MORE: FOLLOW US ON SOCIAL



RECENT CSIAC TIs

- How can the smart city concept be applied to military bases, and what security concerns would need to be assessed?
- Have AI programs like ChatGPT or AskSage been used by military personnel to write awards or decorations and, if so, how can I replicate their success?
- What is the latest guidance on cybersecurity supply chain risk management?

RECENT DSIAC & HDIAC TIs

- What information and documents exist for the DoD's Replicator Initiative?
- How does the military assess risks for autonomous weapons systems?
- What EPCRA Sections 301-303 plans are publicly available, and what are the homeland security risks to making them public?

FEATURED NEWS

AI Cyber Challenge Opens Registration, Adds \$4 Million in Prizes, Shows Scoring Algorithm and Challenge Exemplar

DARPA seeks participants for upcoming competitions to develop artificial intelligence-enabled cyber reasoning systems that can automatically find and fix software vulnerabilities in real-time and at scale in widely... [READ MORE](#)

RECENT NEWS



CISA Issues Request for Information on Secure by Design Software Whitepaper

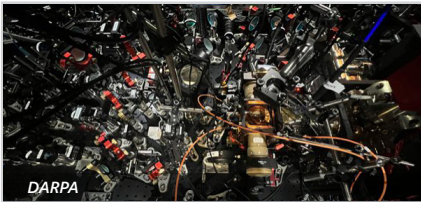
Cybersecurity and Infrastructure Security Agency



U.S. DoD

Trust, Responsibility at Core of DoD Approach to AI

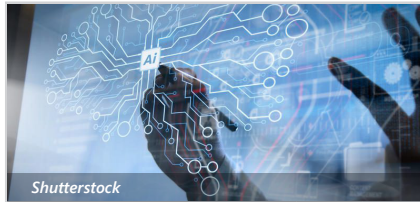
U.S. Department of Defense



DARPA

DARPA-Funded Research Leads to Quantum Computing Breakthrough

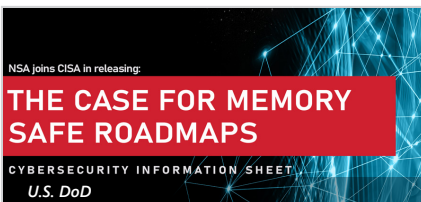
Defense Advanced Research Projects Agency



Shutterstock

NIST Calls for Information to Support Safe, Secure, and Trustworthy Development...

National Institute of Standards and Technology



THE CASE FOR MEMORY SAFE ROADMAPS

CYBERSECURITY INFORMATION SHEET
U.S. DoD

U.S. and International Partners Issue Recommendations to Secure Software Products...

National Security Agency



Securing the Software Supply Chain Recommended Practices for Managing Open Source Software and Software Bill of Materials

Software supply chains are now being targeted throughout their release cycle, from inception through distribution and even after patching. Common methods of compromise used against software supply chains include: exploitation of design flaws, incorporation of vulnerable third party components into a software product, infiltration of the supplier's network with malicious code prior to final software delivery, and injection of malicious software that is subsequently deployed by the customer.

- Evaluate using resources such as the National Vulnerability Database (NVD)
- Follow established guidelines for resilience and vulnerability mitigation
- Monitor sources for defects and vulnerability assessments
- Extract report-related information and dependencies such as cryptographic algorithms
- Perform binary composition analysis to verify the contents prior to shipping
- Run vulnerability scans
- Use SBOM strategies to manage assets and access control

U.S. DoD

NSA and ESF Partners Release Recommended Practices for Managing Open-Source...

National Security Agency



-  Cybersecurity
-  Knowledge Management & Information Sharing
-  Modeling & Simulation
-  Software Data & Analysis

The inclusion of hyperlinks does not constitute an endorsement by CSIA or the U.S. Department of Defense (DoD) of the respective sites nor the information, products, or services contained therein. CSIA is a Defense Technical Information Center (DTIC)-sponsored Information Analysis Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government or CSIA.

4695 Millennium Drive Belcamp, MD 21017
443-360-4600 | contact@csiac.org | csiac.org
Unsubscribe | Past Digests



Cybersecurity & Information Systems
Information Analysis Center