CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // September 3, 2024

THE DOD CYBERSECURITY POLICY CHART

The goal of the DoD Cybersecurity Policy Chart is to capture the tremendous scope of applicable policies, some of which many cybersecurity professionals may not even be aware of, in a helpful organizational scheme. The use of colors, fonts, and hyperlinks is designed to provide additional assistance to cybersecurity professionals navigating their way through policy issues in order to defend their networks, systems, and data.

Click here to download the latest version: https://csiac.org/resources/the-dod-cybersecurity-policy-chart/.

DID YOU MISS OUR LAST WEBINAR?

"Research Challenges for Large Pretrained Models"

WATCH NOW!

or download the slides

NOTABLE TECHNICAL INQUIRY

What is the state of industry investment in developing products in support of counter-artificial intelligence offensive tools and techniques?

The Cybersecurity & Information Systems Information Analysis Center performed open-source research and obtained white papers and reports from numerous sources to include the Defense Technical Information Center Research and Engineering Gateway and Elsevier's ScienceDirect. Overall, the research showed that the best way to counter artificial intelligence (AI) offensive tools was with AI defensive tools. The resulting research is described in detail. **READ MORE**

UPCOMING WEBINAR

Do I Need Cybersecurity Maturity Model...

September 4, 2024
12:00 PM – 1:00 PM

Presenter(s): *Peter Bagley* ***Host:*** *CSIAC*

On November 2010, President Obama issued Executive Order 13556 that formed the controlled unclassified information (CUI) program. Six years later, the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 was published, establishing requirements for CUI, making contractor information systems subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171,... **READ MORE**

CISA

HIGHLIGHT

CISA Releases Secure by Demand Guide

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) released the “Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem,” which helps organizations buying software better understand their software manufacturers approach to cybersecurity and ensure that secure by design is one of their core considerations. **LEARN MORE**

EVENTS

14th Annual Peak Cyber Symposium
September 10–12, 2024
Colorado Springs, CO

AI4SE & SE4AI Workshop 2024
September 17–18, 2024
Arlington, VA

28th Annual IEEE High Performance Extreme Computing Virtual Conference
September 23–27, 2024
Virtual

2024 National Cyber Summit
September 24–26, 2024
Huntsville, AL

TechNet Indo-Pacific
October 22–24, 2024
Honolulu, HI

GridSecCon 2024
October 22–25, 2024
Minneapolis, MN

Want your event listed here?
Email contact@csiac.org to share your event.

VOICE FROM THE COMMUNITY

Thomas Burns
Engineering Manager, Kawasaki Railcar, Inc.

Thomas Burns is an engineering manager in operational technology for Kawasaki Railcar, where he oversees cybersecurity in the global supply chain. He acquires embedded software within the systems for integration into fleets of passenger railcars and tests electromagnetic interference/compatibility. He also manages software requirement compliance and ensures best practices are followed as outlined by the Software Engineering Institute and the Information Systems Audit and Control Association’s Capability Maturity Model Integration framework.

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

Getty Images

RECENT CSIAC TIs

- What integrated priority list needs have the combatant commands submitted for civilian harm mitigation and response capabilities?
- What information exists for the ChatSurfer software, and who is its government point of contact?
- What is the effect of collaborative gaming on team building, cohesion, and culture?

RECENT DSIAC & HDIAC TIs

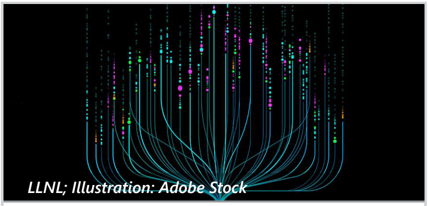
- Can information be provided to explain beamforming techniques used for active, electronically scanned array radar/beam form/beam steer?
- Can live-fire-like training for research and development be provided for the engineers working on weapons platforms at U.S. Army Picatinny Arsenal, NJ?
- What multifunctional robotics platforms are used for first responder applications?

FEATURED NEWS

Keeping Our Seaports Cyber Secure

A new cutting-edge Control Environment Laboratory Resource (CELR) platform developed by the Science and Technology Directorate (S&T) and Cybersecurity and Infrastructure Security Agency (CISA) will help the U.S. Coast Guard (USCG) boost the cyber strength of our nation's...**READ MORE**

RECENT NEWS


LLNL; Illustration: Adobe Stock

Evaluating Trust and Safety of Large Language Models

Lawrence Livermore National Laboratory

J. Wang/NIST and Shutterstock

NIST Releases First Three Finalized Post-Quantum Encryption Standards

National Institute of Standards and Technology

DARPA

Eliminating Memory Safety Vulnerabilities Once and for All

Defense Advanced Research Projects Agency

DVIDS/ U.S. Army National Guard

DISA's DoDNet Program Office Drives Progress in the Next Pivotal Phase of Network...

Defense Information Systems Agency

Pexels

DHS S&T Seeks Solutions for Software Artifact Dependency Graph Generation

U.S. Department of Homeland Security

N. Hanacek, B. Hayes/NIST

NIST Releases Second Public Draft of Digital Identity Guidelines for Final Review

National Institute of Standards and Technology

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

The inclusion of hyperlinks does not constitute an endorsement by CSIAC or the U.S. Department of Defense (DoD) of the respective sites nor the information, products, or services contained therein. CSIAC 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 CSIAC.

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

Cybersecurity & Information Systems Information Analysis Center