

CYBERSECURITY & Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // September 19, 2023



JOURNALS ARE BACK!

After a long absence, the CSIAC Journal is returning! We are now accepting abstracts for our first issue and need your help!

This issue will be a general edition covering any of CSIAC's four focus areas.

ABSTRACT DEADLINE:
October 2, 2023

ARTICLE DEADLINE:
October 15, 2023

SUBMIT IDEAS/ABSTRACT:
journal@csiac.org

To view previous CSIAC journals, visit
<https://csiac.org/journals>.

DID YOU MISS OUR LAST WEBINAR?

"Emerging Developments in Cyberlaw"

 WATCH NOW!

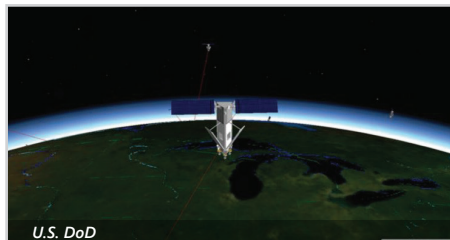
[or download the slides](#)

NOTABLE TECHNICAL INQUIRY

How fast do artificial intelligence (AI)/machine-learning (ML) technologies transition from paper to fielded capability for the People's Republic of China (PRC)?

Cybersecurity and Information Systems Information Analysis Center (CSIAC) subject matter experts from BluePath Labs (BPL) attempted to answer how fast the PRC can transition AI/ML technologies from the lab to the field. Although information was difficult to obtain using open sources, they found that the speed of transition depended on sector and technology. [READ MORE](#)

UPCOMING WEBINAR



**Modeling and Simulation on the
Final Frontier With AFSIM**

October 18, 2023
12:00 PM – 1:00 PM

Presenters: Michael J. Moss, Ph.D. **Host:** CSIAC

This webinar presentation contains CUI and is therefore limited to government and contractors only.

The Advanced Framework for Simulation, Integration, and Modeling (AFSIM) is a government-owned, military simulation framework that enables users to perform complex mission-level simulations for analysis and experimentation. Since 2016, AFSIM's notional space capabilities have been expanded into a fully capable space simulation and delivered to hundreds of... [READ MORE](#)



HIGHLIGHT

Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) warned that cyber actors could target our nation's most sensitive information now and leverage future quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms. This could be particularly devastating to sensitive information with long-term secrecy requirements.

The joint Cybersecurity Information Sheet (CSI), "Quantum-Readiness: Migration to Post-Quantum Cryptography," helps the U.S. Department of Defense, National Security System (NSS) owners, the Defense... [LEARN MORE](#)

EVENTS

National Cyber Summit

September 20–21, 2023
Huntsville, AL

Want your event listed here?

Email contact@csiac.org to share your event.

Gartner IT Infrastructure, Operations & Cloud Strategies Conference

December 5–7, 2023
Las Vegas, NV



VOICE FROM THE COMMUNITY

Tim Watkins

Global Accounts Business Development Manager

Tim Watkins started his U.S. Marine Corps career in 1993. Following 20 years of U.S. Department of Defense experience as a network and cyber engineer, he is now a business development manager focusing on securing control systems and designing defensible architectures for system owners around the world. His work involves prioritizing network and cyber efforts, increasing resiliency, and maturing system owners' plans, policies, and procedures.

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

- What GOTS/COTS software systems can be used to help identify PII with a set of data in a shared drive?
- What survey applications are best to use for gathering survey data from U.S. federal government employees?
- What radar systems does the U.S. Army use that operate at frequencies above 8 GHz?

RECENT DSIAC & HDIAC TIs

- How can UASs detect and deny maritime domain awareness and counter-improvised explosive devices (C-IEDs)?
- What controlled unclassified information documents are available on performing air and missile threat characterization using AI?
- What is the process to submit engine data sheets to JANNAF's Liquid Rocket Engine Database?

FEATURED NEWS

How NETCOM Leads the Army to a Secure Network

FORT HUACHUCA, Ariz. — Zero-trust is a collection of concepts and ideas that assume no trust exists within a defined enterprise network. The Network Enterprise Technology Command (NETCOM) - Army Department of Defense Information Networks, or DoDIN-A, Cybersecurity Strategy... [READ MORE](#)

RECENT NEWS



U.S. Marine Corps

Digital Frontlines: The Marines' Battle in the Virtual Trenches of Cyber Flag 23-2

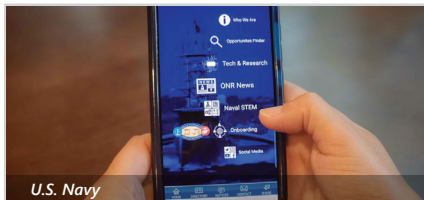
U.S. Marine Corps



Shutterstock

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers

NIST



U.S. Navy

New ONR Mobile App Available to Download

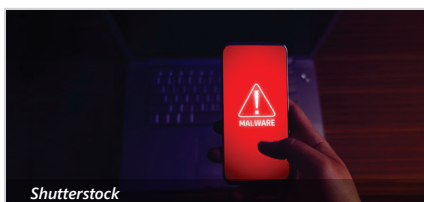
U.S. Navy



U.S. Army

CISA Releases Capacity Enhancement Guide to Strengthen Agency Resilience...

CISA



Shutterstock

U.S. and International Partners Release Report on Russian Cyber Actors Using "Infamous..."

CISA



U.S. Air Force

AFRL's Newest Supercomputer "Raider" Promises to Compute Years' Worth of Data in...

AFRL



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

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

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



Cybersecurity & Information Systems
Information Analysis Center