CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // June 27, 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.

ARTICLE DEADLINE:
July 14, 2023

SUBMIT IDEAS/ABSTRACT:
journal@csiac.org

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

DID YOU MISS OUR LAST WEBINAR?

"Cyber Test and Evaluation (T&E)"

WATCH NOW!

or download the slides

NOTABLE TECHNICAL INQUIRY

What common data models exist that allow merging and generating data from different information repositories?

The Cybersecurity and Information Systems Information Analysis Center (CSIAC) was asked to provide information on the development of common data models that allow merging and generating data from different information repositories. The inquirer was seeking this information to provide context on how their organization's scientific and technical information collection... **READ MORE**

UPCOMING WEBINAR

NIST

NIST Risk Management Framework

July 12, 2023 12:00 PM – 1:00 PM

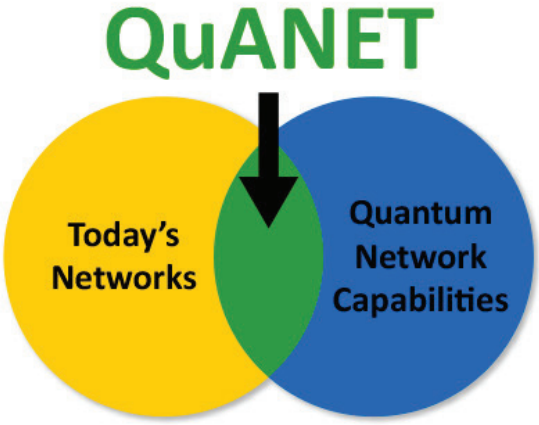
Presenter: *Eduardo Takamura, Jeremy Licata* ***Host:*** *CSIAC*

The NIST Risk Management Framework (RMF) provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. Executing the RMF tasks provides senior leaders... **READ MORE**

FUTURE WEBINARS

Emerging Developments in Cyberlaw

August 9, 2023 12:00 PM – 1:00 PM



DARPA

HIGHLIGHT

A Network Security Revolution Enhanced by Quantum Communication

Can you blend the best of both classical and quantum communications to produce a scalable, vastly more secure networking infrastructure?

That is the question DARPA seeks to answer through its Quantum-Augmented Network (QuANET) program. **LEARN MORE**

EVENTS

Quantum for International Workshop
June 27–29, 2023
Rome, NY

NLIT Summit 2023
June 27–30, 2023
Milwaukee, WI

Zero Trust Government Symposium
July 19–20, 2023
National Harbor, MD

DataConnect Conference
July 20–21, 2023
Columbus, OH

Digital Forensics for National Security Symposium
August 2–3, 2023
College Park, MD

Black Hat USA 2023
August 5–10, 2023
Las Vegas, NV

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

VOICE FROM THE COMMUNITY

William Bryant
Technical Fellow, Modern Technology Solutions, Inc.

Bill "Data" Bryant is currently supporting the DOT&E to incorporate weapon systems cyber effects into existing Cyber Assessment Program analyses of COCOM exercises. He has a diverse background in operations, engineering, planning, and strategy. He codeveloped Aircraft Cyber Combat Survivability and created the Unified Risk Assessment and Measurement Process. He has supported numerous projects to improve cyber survivability, resiliency, and risk assessments on critical cyber-physical systems across multiple 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!

U.S. Department of Justice

RECENT CSIAC TIs

- What are the TRL-9 available capabilities that can detect common tracking devices?
- Can you provide a list of providers who can test and certify open-source software?
- What policies or publications detail what authorities cybersecurity service providers (CSSPs) have?

RECENT DSIAC & HDIAC TIs

- What are the current U.S. Department of Defense capabilities in standoff threat detection using passive sensors?
- What small form factor EA payloads can degrade the performance of peer or near-peer military systems?
- What companies dealing in lithium-ion batteries in the DoD supply chain are sole source or single qualified, and what technologies are considered dual use?

FEATURED NEWS

CISA and FBI Release Advisory on CL0P Ransomware Gang Exploiting MOVEit Vulnerability

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) published a joint Cybersecurity Advisory (CSA) with recommended actions and mitigations... **READ MORE**

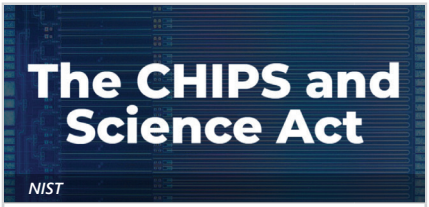
RECENT NEWS

NSA and Coauthors Recommend Best Practices to Secure Remote Access Software

NSA

AFMC Innovation Team Revolutionizing Stealth Fighter Fleet

USAF



U.S. Department of Commerce Announces CHIPS for America R&D Leaders

NIST

New AI Model Aims to Plug Key Gap in Cybersecurity Readiness

PNNL

DARPA's SafeDocs Creates Safer Documents for Safer Computing

DARPA

AFRL Demonstrates New Augmented Reality Capability to Improve DAF Nondestructive Inspections

AFRL

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

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

CSIAC Cybersecurity & Information Systems Information Analysis Center