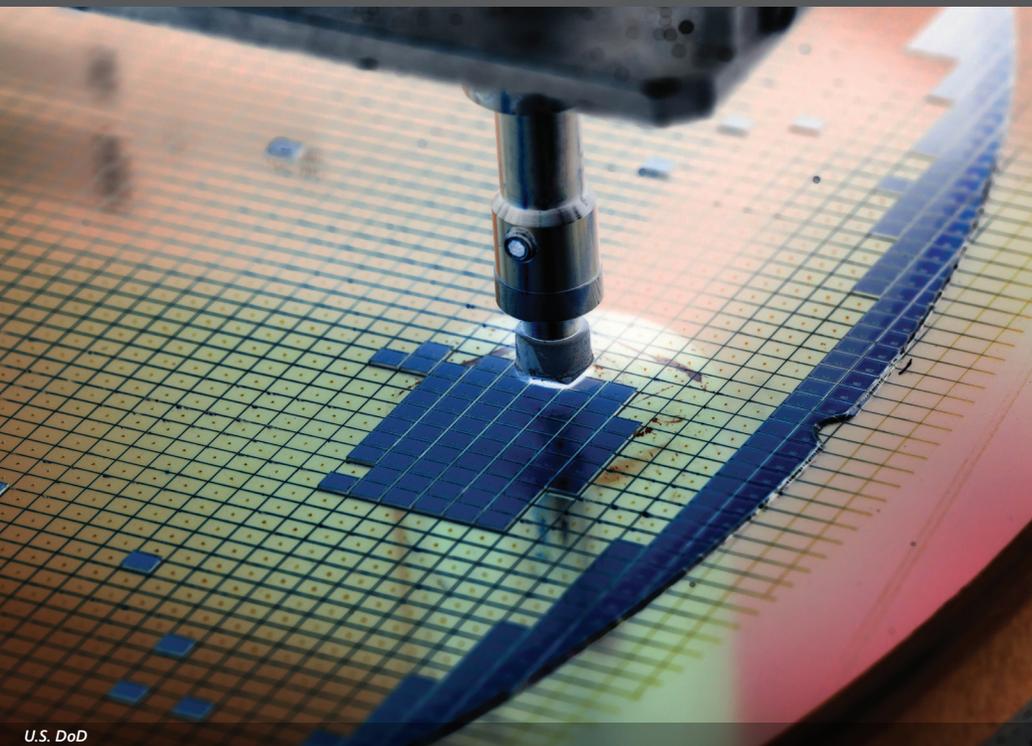


# CYBERSECURITY & Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // February 21, 2023



U.S. DoD

## NOTABLE TECHNICAL INQUIRY

---

### **What is the current state of the art in microelectronics and its impact on the DoD?**

Cybersecurity and Information Systems Analysis Center subject matter experts, experienced with delivering presentations to senior leadership on technical topics, conducted open-source research for relevant information on microelectronics and its impact on the U.S. Department of Defense (DoD). Per the inquirer's request, they compiled the information into a PowerPoint presentation on several subtopics, including DoD importance... [READ MORE](#)



## SNEAK PEEK

---

### **UPCOMING WEBINAR:**

*Understanding Distributed and Blockchain End-to-End Encryption Communication Services*

### **DATE:**

March 15, 2023

### **TIME:**

12:00 PM

### **PRESENTED BY:**

Keven Hendricks

### **HOST:**

CSIAC



## VOICE FROM THE COMMUNITY

### Gary L. Bingham

*Logistics Cataloging and Data Solutions Team Lead, Defense Logistics Agency (DLA)*

Gary Bingham is an experienced team lead with a diverse technical background supporting human resources and logistical systems from requirements to deployment. He is currently involved in supporting DLA's transformation effort for the Federal Logistics Information System. With 30+ years of experience, he has been an end user, developer, supervisor, and contract officer's technical representative.

## 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 an SME!

Join our team today!

**BECOME A SUBJECT  
MATTER EXPERT**



## HIGHLIGHT

### DoD Artificial Intelligence Agents Successfully Pilot Fighter Jet

A joint U.S. Department of Defense (DoD) team executed 12 flight tests in which artificial intelligence (AI) agents piloted the X-62A Variable Stability In-Flight Simulator Test Aircraft (VISTA) to perform advanced fighter maneuvers at Edwards Air Force Base, CA, on December 1-16, 2022. Supporting organizations included the U.S. Air Force Test Center, the Air Force Research Laboratory (AFRL), and the Defense... [LEARN MORE](#)

## FEATURED NEWS

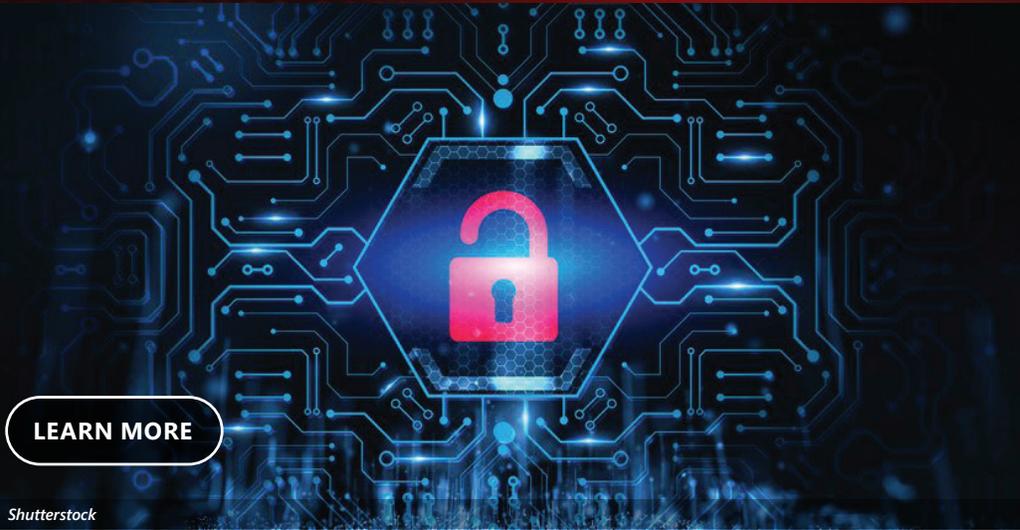
### Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

The Networking and Information Technology Research and Development (NITRD) program's National Coordination Office (NCO) is seeking input from the public on the forthcoming 2023 update of the Federal Cybersecurity Research and Development (R&D) Strategic Plan.

According to the February 7 request for information, the updated plan will be used to guide and coordinate federally funded research in cybersecurity, including... [READ MORE](#)



00111000 00100011 00110101 00100



[LEARN MORE](#)

Shutterstock

## WEBINARS

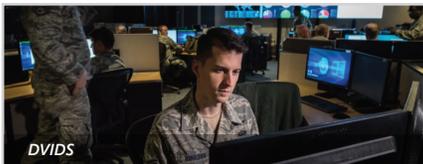
### Understanding Distributed and Blockchain End-to-End Encryption Communication Services

*Presented:* March 15, 2023 12:00 PM - 1:00 PM

*Presenter:* Keven Hendricks

*Host:* CSIAC

Blockchain, cryptocurrency, and “web3” are all terms that you may have heard before or possibly dabbled in; but are you aware that there are dark nets and end-to-end encryption messaging services built on blockchains? Are you familiar with decentralized and distributed encrypted messaging platforms like Tox Chat and Matrix? [LEARN MORE](#)



DVIDS

### Improving Cyber Survivability for Weapon System Mission Assurance

April 13, 2023 12:00 PM



DVIDS

### Systems Security Engineering (SSE) Cyber Guidebook (SSECG)

May 9, 2023 12:00 PM

## EVENTS

### Rocky Mountain Cyberspace Symposium 2023

February 20–23, 2023

### Military Virtual Training & Simulation Summit

February 22–23, 2023

### Software Understanding for National Security Workshop 2023

March 6–10, 2023

### 18th International Conference on Cyber Warfare and Security (ICWS)

March 9–10, 2023

### Global Cyber Innovation Summit

March 29–30, 2023

### MODSIM World 2023

May 22–23, 2023

### Want your event listed here?

Email [contact@csiac.org](mailto:contact@csiac.org), to share your event.

## DID YOU MISS OUR LAST WEBINAR?

“Simulation-Based Testing for DoD Software”

[WATCH NOW!](#)

[or download the slides](#)



-  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 | info@csiac.org | csiac.org  
 Unsubscribe | Past Digests



## RECENT NEWS

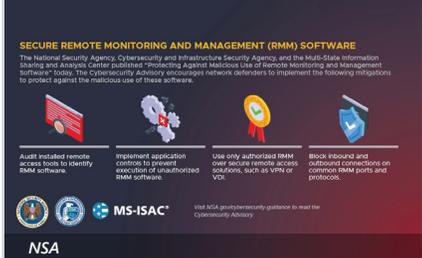


**APPLIED AI CHALLENGE + HEALTHCARE**

GSA

**GSA Applied AI Healthcare Challenge**

GSA 



**SECURE REMOTE MONITORING AND MANAGEMENT (RMM) SOFTWARE**

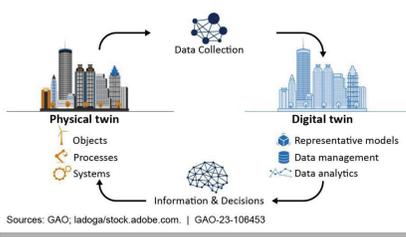
The National Security Agency, Cybersecurity and Infrastructure Security Agency, and the Multi-State Information Security and Analysis Center published "Protecting against malicious use of remote monitoring and management software" today. The Cybersecurity Advisory encourages network defenders to implement the following mitigations to protect against the malicious use of these software.

-  Audit installed remote access tools to identify RMM software.
-  Implement application controls to prevent execution of unauthorized RMM software.
-  Use only authorized RMM client-side remote access solutions, such as VPN or VNC.
-  Block inbound and outbound connections on common RMM ports and protocols.

NSA

**NSA, CISA, and MS-ISAC Release Guidance for Securing Remote Monitoring and Management Software**

NSA  



**Digital Twins—Virtual Models of People and Objects**

Sources: GAO; ladoga/stock.adobe.com. | GAO-23-108453

GAO

**Digital Twins—Virtual Models of People and Objects**

U.S. Government Accountability Office  



**NATIONAL CRYPTOLOGIC MUSEUM**

NSA

**National Cryptologic Museum Unveils Temporary Valentine's Day Exhibit**

NSA 



**Management Advisory: The DoD's Use of Mobile Applications**

DoD Office of Inspector General 



**Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities**

CISA 