CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // November 2, 2021

SUBMIT A TECHNICAL INQUIRY

Shutterstock

NOTABLE TECHNICAL INQUIRY

What are the major requirements of the Cybersecurity Maturity Model Certification for DoD contractors and subcontractors?

In response to the repeated attacks on the U.S. Department of Defense (DoD) supply chain, the release of the Cybersecurity Maturity Model Certification (CMMC) introduces a verification mechanism that will ensure the necessary security mechanisms are in place to better protect Controlled Unclassified Information (CUI) and other sensitive data made available to contractor organizations. CMMC was developed from the contributions of multiple organizations and entities, including the Office of the Under Secretary of Defense for Acquisition and... **READ MORE**

SNEAK PEEK

UPCOMING WEBINAR:
The Case for a National Cybersecurity Safety Board

DATE:
November 4, 2021

TIME:
12:00 PM

PRESENTED BY:
Christopher Hart, Scott Shackleford

HOST:
CSIAC

VOICE FROM THE COMMUNITY

Glyn Gowing
Professor, LeTourneau University

Dr. Gowing is a full-time professor at LeTourneau University, having earned his Ph.D. in computer information systems and specializing in cybersecurity, at Nova Southeastern University. His research interests and experience include malware, penetration testing, reverse-engineering, and forensics. He has experience with multiple processor architectures and operating systems and is currently researching ways to take control of remotely piloted aircraft to protect U.S. troops and our borders from hostile actors. He is a Federal Aviation Administration-certificated commercial drone pilot.

BECOME A SUBJECT MATTER EXPERT

U.S. Department of Defense

HIGHLIGHT

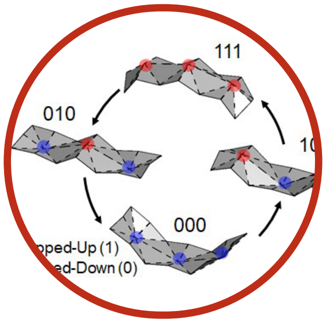
Department of Defense publishes Cyber Table Top Guide Version 2.0

The Cyber Table Top (CTT) method is a type of mission-based, cyber risk assessment that defense programs can use to produce actionable information on potential cyber threats across a system's acquisition life cycle. Actionable information includes potential system vulnerabilities, demonstrated means of exploitation of those vulnerabilities, and an assessment of the resulting mission impacts. CTT is a tool intended to increase understanding of the cyber warfare domain for any system (i.e., business, logistic, or weapon system) in a mission context to help programs better allocate engineering and testing resources.

LEARN MORE

FEATURED NEWS

U.S. Air Force and University Scientists Share Their Vision for Unconventional Computing



Conventional computing hardware represents information as ones and zeros, depending on the state of electronic transistors. This creates artificial bottlenecks in the flow of information processing by first requiring that environmental loads be converted into an electronic state and second by routing the information to centralized computers for processing. Researchers from Wright-Patterson's Air Force Research Laboratory, along with collaborators from the University of Pennsylvania, University of York and... **READ MORE**

Image: U.S. Air Force

LEARN MORE

U.S. Agency for Global Media

WEBINARS

The Case for a National Cybersecurity Safety Board

Presented: *November 4, 2021 12:00 PM - 1:00 PM*
Presenter: *Christopher Hart, Scott Shackleford*
Host: *CSIAC*

In the wake of a series of destabilizing and damaging cyberattacks, there has been a growing call for the U.S. government to establish an analogue of the National Transportation Safety Board (NTSB) to investigate cyberattacks. As we recently argued in a letter to the Wall Street Journal, we think that it is past time for such a move. The SolarWinds hack, for example, highlights many vulnerabilities that have gone unaddressed for too long. First, it shows that the nation's approach to supply chain cybersecurity is notoriously inadequate. Second, it demonstrates that a go-it-alone strategy to cybersecurity risk management is doomed to failure. Cybersecurity firm FireEye's coming forward helped ring the alarm that U.S. early-warning sensors reportedly missed. Third, it highlights the extent to which our nation's critical infrastructure remains vulnerable, despite decades of efforts aimed at improving our defenses. **LEARN MORE**

Shutterstock

Action Bias and the Two Most Dangerous Words in Cybersecurity

December 7, 2021
12:00-12:45 PM

EVENTS

I/ITSEC 2021

November 29-December 3, 2021

DoDIIS Worldwide

December 5-8, 2021

MORS Emerging Techniques Forum

December 7-9, 2021

SANS Cyber Defense Initiative

December 13-18, 2021

Optical Architectures for Displays and Sensing in Augmented, Virtual, and Mixed Reality (AR, VR, MR)

January 23-25, 2022

RSA Conference

February 7-10, 2022

Insider Threat Day at JHU/APL

February 23, 2022

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

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

Cybersecurity & Information Systems Information Analysis Center

RECENT NEWS

Shutterstock

Two Individuals Sentenced for Providing "Bulletproof Hosting" for Cybercriminals

Cybersecurity

Shutterstock

Summit Highlights DoD's Cybersecurity Initiatives, Challenges

Cybersecurity

Shutterstock

Americans Need a Bill of Rights for an AI-Powered World

Knowledge Management & Information Sharing

NNCoE

Securing the Industrial Internet of Things

Cybersecurity

DVIDS

CISA, FBI, and NSA Release Joint Cybersecurity Advisory on BlackMatter Ransomware

Cybersecurity

Avoid Dangers of Wildcard TLS Certificates and the ALPACA Technique

National Security Agency

CYBERSECURITY INFORMATION SHEET

NSA

Avoid Dangers of Wildcard TLS Certificates, the ALPACA Technique

Cybersecurity