RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary
August 22, 2024

PENTAGON A STEP CLOSER TO CMMC STARTING LINE WITH NEW CONTRACT RULE PROPOSAL

Billy Mitchell | DEFENSESCOOP | August 15, 2024

The Pentagon cleared a major milestone Thursday on the path to instituting its cybersecurity standards program for contractors known as the Cybersecurity Maturity Model Certification 2.0. The Department of Defense submitted a proposed rule that, once approved, would incorporate new cyber requirements into all contracts for vendors who want to do business with the U.S. military that involves sensitive but unclassified information. Under the CMMC 2.0 program, any contractor or subcontractor that does work with the DOD involving what's referred to as controlled unclassified information or federal contract information must obtain — or in some cases self-attest to — one of three levels of CMMC compliance, depending on the sensitivity of the information involved in the work. Specifically, the new proposal, published in the Federal Register, aims to amend the Defense Federal Acquisition Regulation Supplement to implement those cybersecurity requirements in contracts as part of the larger CMMC 2.0 program — which itself is in the middle of the federal rulemaking process kickstarted with a separate rule proposal last December after a previous iteration of the CMMC program with more stringent requirements failed.

Read the full article here.

ADVANCING INTERNATIONAL COOPERATION IN QUANTUM INFORMATION SCIENCE AND TECHNOLOGY

Executive Office of the President of the United States | Subcommittee on Quantum Information Science Committee on Science of the National Science and Technology Council Report | August 2024

Quantum information science and technology (QIST) is a critical and emerging field that could revolutionize the way information is collected, processed, and transmitted. This transformative potential is why QIST is a priority for the Biden-Harris Administration. Due to the many potential societal benefits of QIST, the field is being enthusiastically pursued around the globe. Over the past decade, numerous countries and jurisdictions have launched concentrated initiatives to strengthen their QIST enterprises. These developments have expanded global participation in QIST and have increased the importance of international collaboration. While the United States has supported international cooperation in QIST for decades, opportunities exist to adjust and strengthen its approach that will better position the Nation to both leverage international engagements and advance U.S. priorities related to QIST. The United States should continue to focus international engagements on interactions that impart mutual benefits and are based on scientific inquiry, shared values, and economic promise.

Read the full article here.

CONTINUOUS VETTING ENROLLMENT BEGINS FOR NON-SENSITIVE PUBLIC TRUST FEDERAL WORKFORCE

Defense Counterintelligence and Security Agency | August 12, 2024

The Defense Counterintelligence and Security Agency announced the beginning of phased implementation of Continuous Vetting (CV) services for the Non-sensitive Public Trust (NSPT) population this week. The milestone achievement marks the start of a process that will eventually see more than one million additional personnel enrolled in CV services - ensuring a trusted workforce in near real time through automated records, time and event based investigative activity, and agency-specific information sharing. The NSPT population includes individuals who hold non-national security roles but could pose a higher risk of damage to the integrity or efficiency of the service through misconduct. Positions designated as public trust may involve duties and responsibilities such as rulemaking, public safety and health services, law enforcement, fiduciary requirements or protection of government information systems. CV replaces an existing five-year reinvestigation requirement for this population.

Read the full article here.

BEYOND FUSION: PREPARING FOR SYSTEMS RIVALRY WITH CHINA

Liza Tobin, Addis Goldman, and Katherine Kurata | War on the Rocks | August 13, 2024

In 2007, when former Chinese leader Hu Jintao urged China to pursue "Military-Civil Fusion with Chinese characteristics," few in the United States paid attention, much less anticipated the dilemma that this emerging Chinese strategy would pose to U.S. policymakers. Almost two decades later, as the U.S. government considers further restricting China's access to the advanced semiconductors critical to the AI revolution, military-civil fusion — the Chinese Communist Party's strategy to intentionally blur the lines between military and civilian sectors — lies at the heart of the drama. Previous controls, imposed in 2022 and expanded in 2023, came on the heels of the discovery of U.S. semiconductor technology in a supercomputer engineered to develop hypersonic missiles for the People's Liberation Army. New evidence suggests that U.S. microelectronics technology has also aided Chinese advancements in nuclear weapons, torpedoes, and other military applications.

Read the full article here.

GINA RAIMONDO HAS RESHAPED THE COMMERCE DEPARTMENT FOR TECHNOLOGICAL COMPETITION WITH CHINA.

Rishi Iyengar | Foreign Policy | August 16, 2024

The U.S. secretary of commerce is recovering from a fractured tailbone, but she doesn't know how it happened. "I have no idea!" Gina Raimondo says with an exasperated sigh when I ask, before pointing to the donut pillow that she's about to sit down on for our interview. She adds, "I'm only telling you because I don't want you to think I'm weird." We meet late on a Friday morning in July in Raimondo's office on the fifth floor of the Department of Commerce—one of Washington's largest government buildings, located just off Pennsylvania Avenue and across the street from the White House complex. For the past three-and-a-half years, the proximity between the two buildings has been more symbolic than ever. The Commerce Department has been thrust to the forefront of what is arguably President Joe Biden's biggest geopolitical priority: winning the technological race against China and ensuring U.S. economic and military primacy.

Read the full article here.

THOUSANDS OF CORPORATE SECRETS WERE LEFT EXPOSED. THIS GUY FOUND THEM ALL

Matt Burgess | WIRED | August 18, 2024

If you know where to look, plenty of secrets can be found online. Since the fall of 2021, independent security researcher Bill Demirkapi has been building ways to tap into huge data sources, which are often overlooked by researchers, to find masses of security problems. This includes automatically finding developer secrets—such as passwords, API keys, and authentication tokens—that could give cybercriminals access to company systems and the ability to steal data. Today, at the Defcon security conference in Las Vegas, Demirkapi is unveiling the results of this work, detailing a massive trove of leaked secrets and wider website vulnerabilities. Among at least 15,000 developer secrets hard-coded into software, he found hundreds of username and password details linked to Nebraska's Supreme Court and its IT systems; the details needed to access Stanford University's Slack channels; and more than a thousand API keys belonging to OpenAI customers.

Read the full article here.

HONG KONG CHIP FAB RAISES U.S. RESEARCH SECURITY CONCERNS: REPORT

Nikkei Pak Yiu | NIKKEI Asia | June 18, 2024

A Chinese scientist who worked on developing photonic technology for the U.S. military is now leading a third-generation semiconductor chip production venture in Hong Kong, raising concerns about U.S. research security, according to a defense policy group in Washington. Liao Yitao, a former Boston University researcher, will spearhead a new facility producing chip technology crucial for advanced semiconductors in Hong Kong that is set to be operational this year. Prior to starting the company, Liao received a grant from the U.S. Army Research Laboratory to develop high-efficiency, high-power deep ultraviolet (DUV) LEDs for various defense applications, according to a report by Jamestown Foundation researcher Sunny Cheung. Liao's prior work at Boston University's Photonics Center as a researcher from 2005 developing patented dual-use ultraviolet technology underscored the "complex dynamics of talent mobility, technological transfer, and research security," the report said.

Read the full article here.

DEFENSE/EXPERTS WARN OF NATIONAL SECURITY RISKS FROM CHINESE APPS

James Thompson and Wu Shu-wei | FOCUS TAIWAN | August 12, 2024

Chinese apps are a potential national security risk because of China's authoritarian political system, according to two experts from the Institute for National Defense and Security Research (INDSR). "Information security risks are national security risks," said Tzeng Yi-suo (曾怡碩), an associate research fellow at INDSR's Division of Cyber Security and Decision-making Simulation. "As long as the app is under the jurisdiction of the Chinese government, there will basically be security concerns," he explained. Tzeng told CNA that commercial companies collect data about app users and then use algorithms to tailor relevant information and marketing. This is not a problem in a democratic country governed by the rule of law such as Taiwan, the cyber-security expert said, because if the information involves judicial cases, the government will need to go through certain legal procedures to obtain the information.

Read the full article here.

WHITE HOUSE ISSUES NEW SECURITY RULES FOR FEDERALLY FUNDED RESEARCH

Lindsay McKenzie | The American Physical Society (ASP) | August 14, 2024

Over the past several years, NIH has taken actions to address serious threats to the integrity of NIH-funded research. These actions have resulted in significant reductions in violations of peer review confidentiality, failures in reporting foreign employment and financial support, and failures in providing NIH with legally required access to records and scientific data from foreign subrecipients of primary grantees. Many of the concerning practices that NIH has attempted to address have originated from the government of the People's Republic of China (PRC).

Read the full article here.

US CLINICAL TRIALS IN CHINA QUESTIONED BY US LAWMAKERS

Alexandra Alper | U.S. News | August 20, 2024

A bipartisan group of lawmakers on Tuesday called on the Biden administration to ramp up scrutiny of U.S. clinical trials conducted in China, citing the risk of intellectual property theft and the possibility of forced participation of Uyghurs. Republican John Moolenaar, who chairs the House Select Committee on China, and ranking Democrat Raja Krishnamoorthi said U.S. drug companies have collaborated with Chinese military-run hospitals to conduct hundreds of clinical trials over the last decade, including in Xinjiang, home to China's Uyghur minority group. "Given the historical suppression and medical discrimination against ethnic minorities in this region, there are significant ethical concerns around conducting clinical trials in (Xinjiang)," Moolenaar and Krishnamoorthi wrote in a letter dated Aug. 19 and addressed to Robert Califf, who oversees the FDA.

Read the full article here.

SECURING THE CRITICAL TECHNOLOGY SUPPLY CHAIN AS A FUNCTION OF NATIONAL INTELLIGENCE

Archishman Goswami | Observer Research Foundation (ORF) | August 21, 2024

What unites Byzantium, Woodrow Wilson, and Beethoven?

Around 550 CE, Byzantine emperor Justinian I's efforts to produce silk—a highly valued luxury commodity—within the confines of his empire, and thus break the Chinese and Persian monopolies over its production and export, finally bore fruit when silkworms and secret methods of silk production were smuggled over from China by two travelling Indian monks.[1] In 1914, during the First World War, United States (US) President Woodrow Wilson, frustrated by his inability to prohibit US arms manufacturers from selling their wares to European powers, regretted that he "could do nothing else than leave the matter to settle itself", as "the sales proceed from so many sources, and my lack of power is so evident."[2]

Read the full article here.

USEFUL RESOURCES

THE INNOVATION RACE: US-CHINA SCIENCE AND TECHNOLOGY COMPETITION AND THE QUANTUM REVOLUTION

Brandon Kirk Williams | Wilson Center | 2022-2023

Technology competition is the fundamental driver of long-term US-China strategic competition. Technology racing will define the bilateral rivalry over the coming decades, and it is an innovation marathon that American policymakers must navigate to preserve the United States' security and economic competitiveness. After taking power in 2012, Xi Jinping launched a determined campaign to shift the vital center of science and technology (S&T) from the United States to China by pioneering emerging technologies such as quantum. Quantum technologies offer revolutionary potential to upend the geopolitical balance of power. Chinese champions are shifting away from deep investments in quantum communication to keep pace with American progress in quantum computing and sensing. In the next decade, quantum technologies will enter a new stage of maturity that will have the potential to disrupt economies and security.

View the full resource here.

CLOUD COMPUTING: RISK CONSIDERATIONS

National Counterintelligence and Security Center | May 2024

Cloud computing has revolutionized the way government and private sector organizations access, manage, and store data. The migration to cloud technology offers faster innovation, flexible resources, and economies of scale. On the other hand, cloud platforms also present organizations with risk complexities that should be considered from insider threat and Operations Security (OPSEC) perspectives. Whether operating in a traditional, physical computing infrastructure, or in a cloud-based virtual environment, a malicious insider has the capacity to misuse their access, compromise data integrity, and exfiltrate sensitive information.

View the full resource here.

'IS ACADEMIC FREEDOM THREATENED BY CHINA'S INFLUENCE ON U.S. UNIVERSITIES?': ROBERT DALY TESTIFIES BEFORE THE HOUSE FOREIGN AFFAIRS SUB-COMMITTEE ON AFRICA, GLOBAL HEALTH, GLOBAL HUMAN RIGHTS AND INTERNATIONAL ORGANIZATIONS

Robert Daly | Wilson Center | July 1, 2015

Is academic freedom threatened by China's influence on American universities? The history of U.S.-China educational relations suggests that we should first ask whether China has such influence at all. Beginning in 1854, when Yung Wing became the first Chinese student to graduate from an American university, influence has flowed almost entirely in the other direction: from the United States to China. Qing Dynasty students who came to New England as part of the Chinese Educational Mission in 1872 and the nearly 40,000 Chinese who studied here between 1870 and 1949 returned to China with knowledge and ideas that built Chinese industry and sparked calls for liberal social change.

View the full resource here.

RESEARCH SECURITY POLICIES: AN OVERVIEW

Emily Blevins and Marcy Gallo | Congressional Research Service | February 8, 2024

The international scientific community generally views the free and open exchange of information as vital to the process of scientific inquiry, including the vetting of ideas and the verification of research results. The U.S. research ecosystem broadly operates on these principles. Sources have documented a variety of mechanisms employed on behalf of foreign governments—most notably the People's Republic of China—to influence and exploit the openness of the U.S. research ecosystem. The acquisition of U.S. advances in science and technology, intellectual property, and talent by strategic competitors may pose a risk to U.S. national defense and global economic competitiveness. Congress and the executive branch have taken several actions to try to maintain the benefits of an open research ecosystem while attempting to protect it from external threats.

View the full resource here.

DEFENSE PRIMER: QUANTUM TECHNOLOGY

Kelley Sayler | Congressional Research Service | August 14, 2024

Quantum technology translates the principles of quantum physics into technological applications. In general, quantum technology has not yet reached maturity; however, it could hold significant implications for the future of military sensing, encryption, and communications, as well as for congressional oversight, authorizations, and appropriations.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute