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

Open Source Media Summary

February 15, 2024

OSTP ISSUES UPDATED GUIDANCE TO SUPPORT A SECURE AND FAIR RESEARCH ECOSYSTEM

The White House | Office of Science and Technology Policy | February 14, 2024

Today, the White House Office of Science and Technology Policy (OSTP) released two memoranda aimed at supporting a secure and fair research ecosystem in the United States. These documents offer guidance to federal agencies on conflict disclosure forms as well as foreign talent recruitment programs. In a memorandum on Policy Regarding Use of Common Disclosure Forms, OSTP outlines guidelines on the use of common disclosure forms for federal agencies to use when evaluating proposals. These will help the government identify conflicts of commitment and potential duplication with the work of foreign governments. As required by the bipartisan CHIPS and Science Act, OSTP is also releasing Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs. This guidance provides a definition of foreign talent recruitment programs, guidelines for federal employees regarding foreign talent recruitment programs, and guidelines for individuals involved in malign foreign talent recruitment programs in federal projects.

Read the full article here.

DEFENSE INNOVATION BOARD LOOKS TO LOCK DATA ACCESS IN 'ALL VENDOR AGREEMENTS

Edward Graham | Nextgov/FCW | February 5, 2024

The Pentagon would mandate data access in all vendor contracts under a new legislative requirement recommended by the Defense Innovation Board in its most recent report. The report, which examined the Department of Defense’s data economy, said “the current state of data access within DOD vendor agreements is fragmented and inconsistent” and includes suggested legislative text for the FY2025 National Defense Authorization Act that would "enshrine DOD data access and rights in all vendor agreements.” The DIB — an independent oversight committee that provides technology recommendations to the defense secretary and other senior Pentagon officials — was tasked in October 2023 by David Honey, DOD's undersecretary of defense for research and engineering, to help the department enhance its use of data. The study was cleared for public release on January 23. The report called the Pentagon’s efforts to quickly access and use needed data across the entire department “outdated,” noting that inadequate data access practices are “inhibiting effective interoperability and utilization of data across various platforms” needed to enable the DOD’s Combined Joint All-Domain Command and Control initiative.

Read the full article here.

SHADOW AI IN THE 'DARK CORNERS' OF WORK IS BECOMING A BIG PROBLEM FOR COMPANIES

Rachel Curry | CNBC | February 7, 2024

- When employees send information in and out of an organization with new AI tools, tech gatekeepers often miss important pieces of unsanctioned information until it's too late.
- This is called shadow AI and it poses potential threats that information leaders are trying desperately to rein in.
- But outright bans on AI tools aren't the answer either, say experts. A better approach includes guardrails and education.

Amid the growing hype and usage of artificial intelligence, the uncontrolled use that goes beyond the jurisdiction of IT departments is something that information leaders are trying desperately to rein in. Known as shadow AI, this is the AI usage within a company that occurs "in dark corners," said Jay Upchurch, CIO of data analytics platform SAS.

Read the full article here.

NEW SECURITY MEASURES CURTAILING THE STUDY OF CHINA ALARM EDUCATORS

Jordyn Haime | China File | February 2, 2024

Late last year, The New York Times reported on a new state-level bill in Florida that was creating unintended consequences for prospective Chinese graduate students. The bill restricts universities from accepting grants from or participating in partnerships with seven "countries of concern," including China. Now, it is creating confusion among Florida universities unsure where Chinese graduate students fall under the confines of that law. It may have already succeeded in scaring off talented students who could make important research contributions, and universities have refrained from making offers until the law is clarified, the Times reported. It's not just Florida. Several states, including Texas, Louisiana, Ohio, and Montana, have pursued laws aiming to limit foreign influence, particularly from the Chinese Communist Party (CCP), by specifically targeting exchange and cooperation with students, researchers, and academic institutions.

Read the full article here.

WHAT TO EXPECT IN DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION RULE

Jordan McDonald | GovCIO Media Research | January 22, 2024

The Defense Department's proposed rule released in late December codifying the Cybersecurity Maturity Model Certification (CMCC) Program is one step closer to fruition as it enters a comment period open until Feb. 26. Once finalized, the rule would impact any contractor that handles federal contract information (FCI) and controlled unclassified information (CUI) to prevent cyberattacks in the defense industrial base. The program, dubbed CMMC 2.0, outlines the security controls for all three CMMC security levels, establishes processes for monitoring compliance and defines the roles in ensuring cybersecurity for the federal government, contractors and third parties. The rule applies to all DOD contractors and subcontractors that "process, store or transmit federal contract information (FCI) or controlled unclassified information (CUI) on contractor information systems."

Read the full article here.

DOD UPDATES SECTION 1260H LIST OF CHINESE MILITARY COMPANIES OPERATING DIRECTLY OR INDIRECTLY IN THE UNITED STATES

Jingli Jiang, Thomas J. McCarthy, Kimberly M. Myers, Angela B. Styles, Clete Willems, Katherine P. Padgett, Andrew R. Schlossberg, Matthew D. Hawkins, and Thomas Krueger | Akin | February 5, 2024

- On January 31, 2024, the Department of Defense (DoD) released an update to its list of "Chinese military companies" that are "operating directly or indirectly in the United States" in accordance with the statutory requirement of Section 1260H of the National Defense Authorization Act for Fiscal Year 2021, P.L. 116-283. The revised Section 1260H List is available here.
- While designation on the Section 1260H List alone has no current legal consequences (unlike, e.g., sanctions and export controls restricted party lists), Section 805 of the FY 2024 NDAA, passed in December 2023, imposes new contracting restrictions on DoD with respect to entities on the Section 1260H List or any entity subject to the control of such an entity, which will become effective on June 30, 2026. Implementing regulations for this law are forthcoming by DoD.

Read the full article here.

ANOTHER SECURITY LAW PROPOSED AS ACADEMIC EXODUS CONTINUES

Yojana Sharma | University World News | February 7, 2024

A new local security law proposed by the Hong Kong government specifically under the city's legal system outlines seven national security offences and also adds new 'state secrets' prohibiting disclosure of economic and social information or technology and science deemed to be of importance to the security of Hong Kong or China. Academics fear the new law could constrain research. Academics said such specific references unveiled in the proposed law last week could dramatically affect the way research is conducted in these fields, including international research collaboration under a new crime of 'foreign interference' in Hong Kong and national (China) affairs, for fear of falling foul of possible national security rules. Under Hong Kong's mini constitution, known as the Basic Law, Article 23 requires Hong Kong to enact its own laws to prohibit seven national security offences.

Read the full article here.

CHINESE SECURITY AGENCIES TELL STUDENTS STUDYING ABROAD TO BEWARE RISK FROM FOREIGN SPIES

Sylvie Zhuang | South China Morning Post | February 7, 2024

China's top spy agency has warned Chinese students to be alert to the risk from foreign spies when studying abroad. The warning from the Ministry of State Security comes amid a sweeping national security drive. In a post on the ministry's WeChat account it told the story of a "real case" involving a Chinese graduate who, it claimed, had secured a place from a "top ranking" foreign university despite failing the Chinese college entrance exam in 2006. Do you have questions about the biggest topics and trends from around the world? Get the answers with SCMP Knowledge, our new platform of curated content with explainers, FAQs, analyses and infographics brought to you by our award-winning team. It said the student, identified only by the surname Zhang, had been "severely punished" for his role in leaking Chinese scientific research after graduating.

Read the full article here.

UK MINISTERS ACCUSED OF IGNORING SECURITY THREATS FROM CHINA-LINKED UNIVERSITY PROJECTS

BNN Correspondents | BNN The People's Network | February 7, 2024

UK ministers face accusations of neglecting national security concerns relating to university research projects tied to China. An internal audit highlighted an 'extremely high risk' of sensitive information being accessed by Beijing, with the government seemingly taking no action to mitigate these risks. In a revelation that has sent shockwaves through the corridors of power, UK ministers stand accused of disregarding national security risks arising from university research projects linked to the Chinese state. This alarming information was unearthed during a session of prime minister's questions in the House of Commons, putting the spotlight on the government's approach towards safeguarding national interests. Stewart McDonald, a Member of Parliament from the Scottish National Party (SNP), exposed an internal audit from within Whitehall. The audit flagged an 'extremely high risk' of sensitive data falling into the hands of Beijing.

Read the full article here.

CHINA'S STATE SECURITY AUTHORITY CALLS FOR AWARENESS OF COUNTERESPIONAGE WHEN STUDYING ABROAD

The Global Times | February 7, 2024

China's top anti-espionage authority called for the public to enhance their awareness of counterespionage when studying abroad, after it published a case on its WeChat account on Wednesday, describing a story of an overseas university graduate who was recruited and turned to become a foreign spy by an intelligence agency while studying abroad, and engaged in espionage activities. According to the Ministry of State Security (MSS), a student surnamed Zhang (pseudonym) was admitted to a top-ranked oversea university in 2006 and became the class monitor. He gained the recognition of the school leader named Kaidi (pseudonym), and they became friends despite their age difference. However, it was precisely this "friend" that gradually pushed Zhang into a carefully designed trap by foreign intelligence agencies, causing him to become deeply entangled.

Read the full article here.

US AND CHINA LIKELY TO DELAY RENEWAL OF KEY SCIENCE PACT AGAIN

Natasha Gilbert and Smriti Mallapaty | Nature | February 8, 2024

China and the United States will once again probably delay the renewal of a decades-old pact to cooperate on science and technology. The two nations have been negotiating for the past six months, but need more time to settle new terms and conditions requested by both sides, sources tell Nature. The 45-year-old pact is a symbolic agreement that doesn't provide any funding, but instead lays the groundwork for cooperation on research in a broad range of fields, including health, the environment and energy. Many researchers in the United States and China say that the agreement is crucial to establishing scientific collaborations and building strong research relationships between the two nations. They worry that science will suffer in both countries if the pact is not renewed. “Collaboration is the only way to conquer a lot of the scientific challenges the world is facing today,” says Marina Zhang, who studies innovation with a focus on China at the University of Technology Sydney in Australia.

Read the full article here.

CHINESE UNIVERSITIES' CROSS-BORDER RESEARCH COLLABORATION IN THE SOCIAL SCIENCES AND ITS IMPACT

Yang Liu, Jinyuan Ma, Huanyu Song, Ziniu Qian, and Xiao Lin | Multidisciplinary Digital Publishing Institute (MDPI) | February 1, 2024

This paper examined the coauthorship patterns in Chinese researchers' cross-border research collaboration in the social sciences based on articles and reviews indexed in the Scopus database (2010–2019). We explored the evolution of coauthorship patterns by proportion of collaboration, year, research field, country/region, and research institution; additionally, the quality/impact of the coauthored publications was examined using four levels of paper quality (Q1–4), citations per paper, and FWCI. We found that collaboration between Chinese and international scholars is very common, and more than 40% of all papers published by Chinese scholars from 2010 to 2019 involved cross-border collaboration. The growth in collaboration was very steady over the past 10 years, increasing by an average of 20% per year. United States scholars are the most common research collaboration partners for Chinese scholars in the social sciences, followed by those in Hong Kong, the United Kingdom, Australia, and Canada.

Read the full article here.

THAT COLLEAGUE OR CUSTOMER ON ZOOM MIGHT BE AN AI DEEPFAKE. HERE'S HOW YOU CAN TELL

Minda Zetlin | INC.Com | February 8, 2024

Artificial intelligence is increasingly used to create elaborate scams in which a real person's voice and sometimes video image is used to convince an unsuspecting colleague, friend, or even family member that a request for funds or sensitive information is legitimate. Anyone can be deepfaked--even Taylor Swift. But there are a few things you can do to protect yourself and your company. The world suddenly learned about the financial dangers of AI fraud when Hong Kong police reported this week that an unnamed financial institution in lost about $25.6 million ($200 million Hong Kong dollars) after an employee was deceived by an elaborate AI deepfake. The employee had received an email purportedly from the company's UK-based chief financial officer requesting a secret transaction. The employee suspected that the email was a fake--but then attended a video meeting with the CFO and several other top executives who all looked and sounded like his real bosses. Convinced, the employee made the transaction. But no one on the call actually was who they appeared to be.

Read the full article here.

GOODBYE SF-86? OMB APPROVES NEW 'PERSONNEL VETTING QUESTIONNAIRE'

Justin Doubleday | Federal New Network | February 9, 2024

The Standard Form-86, a long-used questionnaire for government positions requiring security clearance, is set to be phased out after the White House Office of Management and Budget approved a new form replacing the SF-86 and several other legacy forms. OMB approved the Personnel Vetting Questionnaire (PVQ) in November, according to the latest quarterly update on the "Trusted Workforce 2.0" initiative from the Performance Accountability Council. The questionnaire consolidates the SF-86, "Questionnaire for National Security," along with several other vetting questionnaires used for federal jobs, including public trust and non-sensitive positions. The Defense Counterintelligence and Security Agency is now working on plans to integrate the PVQ into the new "eApp" web portal for background investigation applications.

Read the full article here.

USEFUL RESOURCES

TECHNOLOGY & NATIONAL SECURITY

Center for a New American Security (CNAS)

Technology is changing our lives. Rapid developments in artificial intelligence, autonomy and unmanned systems, digital infrastructure, networking and social media, and disinformation are profoundly altering the national security landscape. Nation-states have new tools at their disposal for political influence as well as new vulnerabilities to attacks. Authoritarian governments are empowered by high-tech tools of oppression and exploit radical transparency. Artificial intelligence and automation raise profound questions about the role of humans in conflict and war. CNAS' Technology and National Security program explores the policy challenges associated with these and other emerging technologies. A key focus of the program is bringing together the technology and policy communities to better understand these challenges and together develop solutions.

Read the full article here.

CURRENT AND EMERGING TECHNOLOGIES IN U.S.-CHINA ECONOMIC AND NATIONAL SECURITY COMPETITION

The U.S.-China Economic and Security Review Commission | February 1, 2024

The hearing examines national security risks created by the sale of Chinese IT hardware and software in the U.S. as well as potential tools to regulate their use, China's research in military applications of AI and quantum information science, and China's progress in AI, bio-technology, and battery technology.

Read the full article here.

ROR IS A GLOBAL, COMMUNITY-LED REGISTRY OF OPEN PERSISTENT IDENTIFIERS FOR RESEARCH ORGANIZATIONS

The Research Organization Registry (ROR)

The Research Organization Registry (ROR) is a global, community-led registry of open persistent identifiers for research organizations. ROR makes it easy for anyone or any system to disambiguate institution names and connect research organizations to researchers and research outputs. Organizations are not static entities. They change their names, merge, split, shut down, and re-emerge, and this makes it difficult to connect research organizations to research outputs and researchers. A persistent identifier for research organizations makes this easier.

Read the full article here.

EVENTS OF NOTE

REMINDER: 2024 ASCE ANNUAL SEMINAR TO BE HELD MARCH 4-8, AT TEXAS A&M UNIVERSITY

Now in its eighth year, the annual ASCE Seminar has become the premier event for training, networking, and collaboration specifically targeted at the academic research enterprise. For ASCE 2024, we expect over 400 participants from various federal agencies, more than 150 universities, and 15 countries.

View the full resource here.

GLOBAL CHINA HUB

Atlantic Council

The Global China Hub is hosting an in-person public conference on February 21 and February 22 looking at China in the Global South. After decades of being relegated to the periphery of China's geostrategy, the regions of what is now collectively termed the Global South have become an essential component of China's external engagement and foreign policy. China is now a central player in the economic and technological development of countries across the developing world, with significant implications for these countries' trajectories as well as their relations with the United States and other developed democracies. At the same time, China's growing influence in these regions is increasingly hampered by systemic factors. These dynamics all play out against the backdrop of escalating Sino-US strategic economic, security and technological rivalry, and transnational security threats like pandemics, climate change, and terrorism.

Read the full article here.

RESEARCH SECURITY OPPORTUNITIES

THE UNIVERSITY OF MISSOURI IS PLEASED TO ANNOUNCE OPENING FOR A FACILITY SECURITY OFFICER (FSO) POSITION

More information here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute