ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 10, 2023

FACT SHEET: BIDEN-HARRIS ADMINISTRATION ANNOUNCES NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY

The White House | May 4, 2023

Today, the Biden-Harris Administration released the United States Government's National Standards Strategy for Critical and Emerging Technology (Strategy), which will strengthen both the United States' foundation to safeguard American consumers' technology and U.S. leadership and competitiveness in international standards development. Standards are the guidelines used to ensure the technology Americans routinely rely on is universally safe and interoperable. This Strategy will renew the United States' rules-based approach to standards development. It also will emphasize the Federal Government's support for international standards for critical and emerging technologies (CETs), which will help accelerate standards efforts led by the private sector to facilitate global markets, contribute to interoperability, and promote U.S. competitiveness and innovation. The Strategy focuses on four key objectives that will prioritize CET standards development: Investment: Technological contributions that flow from research and development are the driving force behind new standards.

Read the full article here.

DEAR COLLEAGUE LETTER: A REQUEST FOR INPUT ON THE DEVELOPMENT OF THE U.S. RESEARCH SECURITY AND INTEGRITY INFORMATION SHARING ANALYSIS ORGANIZATION

National Science Foundation | May 4, 2023

Dear Colleague: The U.S. National Science Foundation (NSF) requests input from the research community on the development of a Research Security and Integrity Information Sharing Analysis Organization (RSI-ISAO), as mandated by Section 10338(b) of the CHIPS and Science Act of 2022 (Public law 117-167).1 This Dear Colleague Letter (DCL) seeks to solicit feedback, ideas, and proposed recommendations from the research community to ensure the products, services, and tools provided by the RSI-ISAO align with the needs and expectations of the research community. Foreign government interference threatens the U.S. science and technology (S&T) research ecosystem and the U.S. research community by undermining the principles and values foundational to the conduct of research, and the openness necessary for the research enterprise to thrive.

Read the full article here.

FACT SHEET: BIDEN-HARRIS ADMINISTRATION ANNOUNCES NEW ACTIONS TO PROMOTE RESPONSIBLE AI INNOVATION THAT PROTECTS AMERICANS' RIGHTS AND SAFETY

The White House | May 4, 2023

Today, the Biden-Harris Administration is announcing new actions that will further promote responsible American innovation in artificial intelligence (AI) and protect people's rights and safety. These steps build on the Administration's strong record of leadership to ensure technology improves the lives of the American people, and break new ground in the federal government's ongoing effort to advance a cohesive and comprehensive approach to AI-related risks and opportunities. AI is one of the most powerful technologies of our time, but in order to seize the opportunities it presents, we must first mitigate its risks. President Biden has been clear that when it comes to AI, we must place people and communities at the center by supporting responsible innovation that serves the public good, while protecting our society, security, and economy. Importantly, this means that companies have a fundamental responsibility to make sure their products are safe before they are deployed or made public.

Read the full article here.

A NEXT-GENERATION STRATEGY FOR AMERICAN SCIENCE

Frank Lucas | Issues in Science and Technology | Spring 2023

During my tenure in Congress, where I've represented Oklahoma's third district since 1994, I've had the privilege of serving on three committees and working closely with many more. Of these committees, the House Committee on Science, Space, and Technology does not have the highest profile, but it does have one of the most important portfolios. That's because the work done by this committee goes further than addressing the challenges we face today—it paves the way for our long-term development as a nation. America's economic strength, national security, and our quality of life all fundamentally depend on our ongoing scientific progress. In fact, more than 60% of America's economic growth in the last century is due to advances in science and technology. US public investment in research and development adds nearly $200 billion in economic value, and basic research in particular increases long-term productivity across multiple industries.

Read the full article here.

MORE CANADIAN UNIVERSITIES NOW SAY THEY'LL STEER CLEAR OF CHINESE TELECOM HUAWEI

Joanna Chiu | Toronto Star | May 4, 2023

Several top Canadian universities said Thursday they have decided not to enter new research agreements with Huawei, after the University of Waterloo told the Star this week it would end all existing partnerships with the Chinese telecommunications giant. Amid increased scrutiny of Canadian university partnerships, and as a national conversation continues about Beijing's influence efforts in this country, the move by Waterloo was seen as a potentially precedent-setting step. The University of Toronto was among the schools to make a statement Thursday. "In response to concerns about research security, the University of Toronto decided in April to stop any new research engagements with Huawei," said a statement from Leah Cowen, vice-president, research and innovation and strategic initiatives. "This includes new agreements, new projects within existing agreements, renewals and funded extensions. We also hired a Director of Research Security in September 2022, and are in the process of establishing a research security office."

Read the full article here.

TOP US CYBER OFFICIAL WARNS AI MAY BE THE 'MOST POWERFUL WEAPON OF OUR TIME'

Christian Vasquez | CyberScoop | May 5, 2023

Director of the Cybersecurity and Infrastructure Security Agency Jen Easterly warned that artificial intelligence may be both the most "powerful capability of our time" and the "most powerful weapon of our time." "Imagine a world in the not to distant future where how-to guides, AI-generated imagery, auto-generated shopping lists are available for terrorist and for criminals, providing the capability to develop things like cyber weapons, chemical weapons, bio weapons," Easterly said Friday at a security summit at Vanderbilt University in Nashville, Tennessee. "And that's not even the worst case scenario." Reminiscent of her Carnegie Melon speech in February calling on software vendors to stop building insecure-by-design products that maximize profits over safety, Easterly's warns that the potential benefits of AI also comes with severe threats. "So far the cost that we've paid for speed over security is pretty steep but not existential," Easterly said. "But AI is different." The warning from one of the top cybersecurity officials in the Biden administration comes a day after the White House held met with top AI companies over concerns about the seemingly rapid adoption of large language models.

Read the full article here.

PENTAGON CIO WARNS AGAINST PAUSE IN AI DEVELOPMENT

Chris Riotta | FCW | May 4, 2023

John Sherman warned that a pause in U.S. development of AI tools and research could potentially give overseas adversaries an upper hand. A pause in the development of artificial intelligence tools and products in the United States could have troubling consequences in the emerging technology race against countries like Russia and China, a top Defense Department official warned on Wednesday. DOD Chief Information Officer John Sherman spoke out against calls from some leading technologists for a six-month pause in AI development and research, suggesting that implementing a global halt would be virtually impossible and could allow adversaries to continue advancing their own AI initiatives. "Some have argued for a six-month pause, which personally I don't advocate for," Sherman said at a TechNet Cyber event hosted by the nonprofit AFCEA. "If we stop, guess who is not going to stop? Potential adversaries overseas." His comments come after AI and national security experts testified to Congress last month about advancements in emerging technology that are outpacing federal regulation.

Read the full article here.

EXPORT CONTROL AS NATIONAL SECURITY POLICY

Issues in Science and Technology | Spring 2023

In 1909, as part of the Declaration of London on the Laws of Naval War, a group of nations produced a list of items we would today consider "dual use," but at the time were called "conditional contraband." The list was the first time a large set of states had agreed to a common understanding of what goods and technologies represented a security concern. Interestingly, the list included an item that is not on current export control lists, but is very much on the minds of people engaged in security governance today: balloons. Like general aviation airplanes, box cutters, or novel genetic sequences, balloons, such as the ones floating over the United States recently, represent a type of security concern that is not really visible to, and therefore governable by, today's conventional export controls. But they still represent security concerns to the state. In "Change and Continuity in US Export Control Policy" (Issues, Winter 2023), John Krige and Mario Daniels discuss how a historical gaze allows us to better understand "the context, effects, prospects, and challenges of the Biden administration's current policy changes" on export controls.

Read the full article here.

WHY THE U.S. SECURITY-CLEARANCE PROCESS HAS A DIGITAL BLIND SPOT

Vera Bergengruen | Time | May 4, 2023

In Nov. 2020, Jack Teixeira wrote a letter to the local police chief asking him to reconsider allowing him to own guns. The Dighton, Mass., police had denied the 18-year-old's two previous requests for a firearms license, citing an incident when Texeira, as a high-school sophomore, was suspended for alleged violent and racial threats, including comments about guns at school. This time, Teixeira's pleas worked. As a newly minted member of the Massachusetts Air National Guard, he had recently received a top-secret security clearance. "The investigation process was extremely thorough," he wrote to the police chief, arguing that the U.S. government had deemed him qualified to become "a person with a military career in intelligence and a person that now has the national trust to safeguard classified information." That trust turned out to be misplaced. Last month, Teixeira was arrested and charged with posting classified military documents online in the most damaging leak of U.S. intelligence in a decade, revealing sensitive information about the war in Ukraine and complicating relations with U.S. allies.

Read the full article here.

GENERATIVE AI IN CYBERSECURITY: THE BATTLEFIELD, THE THREAT, & NOW THE DEFENSE

Chris Lehman | Unite AI | May 3, 2023

The Battlefield: What started off as excitement around the capabilities of Generative AI has quickly turned to concern. Generative AI tools such as ChatGPT, Google Bard, Dall-E, etc. continue to make headlines due to security and privacy concerns. It's even leading to questioning about what's real and what isn't. Generative AI can pump out highly plausible and therefore convincing content. So much so that at the conclusion of a recent 60 Minutes segment on AI, host Scott Pelley left viewers with this statement; "We'll end with a note that has never appeared on 60 Minutes, but one, in the AI revolution, you may be hearing often: the preceding was created with 100% human content." The Generative AI cyber war begins with this convincing and real-life content and the battlefield is where hackers are leveraging Generative AI, using tools such as ChatGPT, etc. It's extremely easy for cyber criminals, especially those with limited resources and zero technical knowledge, to carry out their crimes through social engineering, phishing and impersonation attacks.

Read the full article here.

THE NSA IS WARNING AI STARTUPS: 'CHINA IS COMING FOR YOU'

Patrick Tucker | Defense One | April 28, 2023

The National Security Agency is telling U.S. tech companies to beware Chinese attempts to steal their AI technology, while the Pentagon's intelligence chief is warning about what China might do with the new tools. "We think much about the ability of what AI is going to do for us in the future. One of the things that we have communicated very clearly to a number of the U.S. companies is the importance of securing the intellectual property that you have invested within this. This type of capability because this will be a target of our adversaries," Gen. Paul Nakasone told the House Armed Services cyber and intelligence subcommittee on Thursday. While the head of the NSA and Cyber Command didn't mention China by name, he didn't have to. Like his predecessors, Nakasone frequently describes China as the top nation-state threat to U.S. intellectual property. The world has been captivated by the rise of new public-facing large language model artificial intelligence programs like ChatGPT, which can provide complex, human-like answers to a wide number of prompts.

Read the full article here.

SAFEGUARDING OUR FUTURE: PROTECTING GOVERNMENT AND BUSINESS LEADERS AT THE U.S. STATE AND LOCAL LEVEL FROM PEOPLE'S REPUBLIC OF CHINA (PRC) INFLUENCE OPERATIONS

The National Counterintelligence and Security Center | July 2022

For decades, a broad range of entities in China have forged ties with government and business leaders at the state and local levels of the United States, often yielding benefits for both sides. However, as tensions between Beijing and Washington have grown, the government of the People's Republic of China (PRC) under President Xi Jinping has increasingly sought to exploit these China-U.S. subnational relationships to influence U.S. policies and advance PRC geopolitical interests. In confronting this challenge, it is important that U.S. state and local leaders not cast blanket suspicion on all outreach from China, given that the threat of exploitation emanates from the PRC government and the Chinese Communist Party (CCP), not the people of China generally and not Chinese Americans, who themselves are often victimized by PRC aggression. In partnering with any foreign entity, U.S. state and local leaders should exercise vigilance, conduct due diligence, and ensure transparency, integrity, and accountability are built into the partnership to guard against potential foreign government exploitation.

Read the full article here.