ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 20, 2021

RECOMMENDED PRACTICES FOR STRENGTHENING THE SECURITY AND INTEGRITY OF AMERICA'S SCIENCE AND TECHNOLOGY RESEARCH ENTERPRISE

Subcommittee on Research Security and the Joint Committee on the Research Environment of the National Science and Technology Council | January 2021

The purpose of this document is to offer recommendations research organizations (e.g., universities, private companies, independent research institutes) can take to better protect the security and integrity of America's research enterprise. It serves as a complementary document to National Security Presidential Memorandum 33 (NSPM-33), titled, "U.S. Government Supported Research and Development National Security Policy." NSPM-33 directs Federal departments and agencies to act to protect federally-funded research, including from foreign interference, and incorporates recommendations that the JCORE Subcommittee on Research Security developed in partnership with the National Security Council staff, working across Federal agencies and informed by inputs from across America's research enterprise, including universities, companies, associations, and scientific societies. The recommendations for research organizations contained in this report were likewise informed by extensive engagement across the U.S. research enterprise and with international partners. These recommendations constitute recommended practices that will strengthen and protect the security and integrity of America's research enterprise.

Read the full report here.

US COUNTER-INTEL CHIEF WARNS BIDEN ADMIN OF CHINA'S MALIGN FOREIGN INFLUENCE: 'ONE OF THE BIGGER CHALLENGES'

Brooke Singman | Fox News | January 19, 2021

National Counterintelligence and Security Center Director Bill Evanina said no country poses a "broader, more severe" threat to America than China, telling Fox News that its malign foreign influence campaign against the United States will be one of the "bigger challenges" for the incoming Biden administration. During an exclusive interview with Fox News, Evanina outlined the threat China poses to the United States -- from big data collection to economic espionage, to malign foreign influence to supply chain and critical infrastructure. "From a threat perspective, Russia is a significant adversary particularly with regard to cyber intrusions, malign influence, and sowing discord in our democracy," Evanina told Fox News. "However, no country poses a broader, more severe intelligence collection threat to America than China."

Read the full article here.

FACT SHEET: NATIONAL SECURITY PRESIDENTIAL MEMORANDUM ON UNITED STATES RESEARCH AND DEVELOPMENT NATIONAL SECURITY POLICY

United States Office of Science and Technology Policy | January 16, 2021

PROTECTING OUR RESEARCH AND DEVELOPMENT ENTERPRISE AGAINST FOREIGN GOVERNMENT INTERFERENCE AND EXPLOITATION:

- President Trump has signed National Security Presidential Memorandum 33 (NSPM-33) to direct a national response to safeguard the security and integrity of Federally funded research and development (R&D) in the United States.
- The NSPM strengthens and standardizes requirements for disclosure of information related to potential conflicts of interest and of commitment from individuals with significant influence on America's R&D enterprise, including individuals leading Federally funded research projects and parties involved in the process of allocating Federal funding.
- Following the signing of the NSPM, the Federal Government will continue to work closely with stakeholders to enhance information sharing and coordination, and to develop education and training resources to strengthen the security and integrity of our R&D enterprise.

Read the full fact sheet here.

MIT PROFESSOR ARRESTED AND CHARGED WITH GRANT FRAUD

U.S. Department of Justice | January 14, 2021

A professor and researcher at Massachusetts Institute of Technology (MIT) was charged and arrested today in connection with failing to disclose contracts, appointments and awards from various entities in the People's Republic of China (PRC) to the U.S. Department of Energy. Gang Chen, 56, was charged by criminal complaint with wire fraud, failing to file a foreign bank account report (FBAR) and making a false statement in a tax return. Chen will make an initial appearance today before Magistrate Judge Donald L. Cabell. According to charging documents, Chen is a naturalized U.S. citizen who was born in China. He is a professor and researcher at MIT where he serves as Director of the MIT Pappalardo Micro/Nano Engineering Laboratory and Director of the Solid-State Solar Thermal Energy Conversion Center (S3TEC). Since approximately 2013, Chen's research at MIT has been funded by more than $19 million in grants awarded by various U.S. federal agencies.

Read the full article here.

NASA SCIENTIST ADMITS TO LYING IN CHINA TRADE SECRETS CASE

Chris Dolmetsch | Bloomberg | January 13, 2021

A senior NASA scientist admitted to lying to authorities about his participation in a program the U.S. says is designed to siphon intellectual property to China. Meyya Meyyappan, of Pacifica, California, pleaded guilty on Wednesday in federal court in New York to one count of making false statements, Acting U.S. Attorney Audrey Strauss in Manhattan said in a statement. Meyyappan, 66, has worked for NASA since 1996 and has been chief scientist for exploration technology at the Center for Nanotechnology at Ames Research Center in California since 2006, according to the statement. Prosecutors said Meyyappan participated in China's Thousand Talents Program, which the U.S. says was established by the Chinese government "to recruit individuals with access to or knowledge of foreign technology or intellectual property," and served as a professor at universities in China, South Korea and Japan.

Read the full article here.

RESEARCHERS DISCLOSE UNDOCUMENTED CHINESE MALWARE USED IN RECENT ATTACKS

Ravie Lakshmanan | The Hacker News | January 15, 2021

Cybersecurity researchers have disclosed a series of attacks by a threat actor of Chinese origin that has targeted organizations in Russia and Hong Kong with malware — including a previously undocumented backdoor. Attributing the campaign to Winnti (or APT41), Positive Technologies dated the first attack to May 12, 2020, when the APT used LNK shortcuts to extract and run the malware payload. A second attack detected on May 30 used a malicious RAR archive file consisting of shortcuts to two bait PDF documents that purported to be a curriculum vitae and an IELTS certificate. The shortcuts themselves contain links to pages hosted on Zeplin, a legitimate collaboration tool for designers and developers that are used to fetch the final-stage malware that, in turn, includes a shellcode loader ("svchast.exe") and a backdoor called Crosswalk ("3t54dE3r.tmp").

Read the full article here.

U.S. EXPORT CONTROL REFORMS AND CHINA: ISSUES FOR CONGRESS

Congressional Research Service | January 14, 2021

Over the past two years, the U.S. government has reformed—through legislation, regulation, and licensing practices—the export control system that regulates dual-use exports (goods and technology that have both civilian and military uses). These changes largely aim to address concerns about China's attempts to seek global civilian and military leadership in advanced and emerging technologies through coordinated industrial policies. Some of these reforms have prompted U.S. business concerns because they tighten technology trade with China, which is a growing market for many firms. Other reforms—such as setting emerging technology controls, expanding controls on existing technologies of concern, and reforming the licensing process—are ongoing. Congress has an important role in overseeing the reforms it legislated and shaping the evolving U.S. export control regime.

Read the full article here.

ZOOM EMPLOYEE: INSIDER THREAT HELPING CHINA

Drew Todd | Secure World | January 9, 2021

A complaint and arrest warrant were recently unsealed in U.S. federal court, charging former Zoom employee Xinjiang Jin, also known as Julien Jin, with several crimes he carried out on behalf of China. Jin worked for U.S.-based Zoom in the People's Republic of China (PRC). The FBI says he helped the PRC reveal political opponents and shut down Zoom meetings that took place in May and June 2020. The meetings involved U.S. citizens and were part of efforts to commemorate the 1989 Tiananmen Square massacre. He also fabricated evidence that hosts and attendees of these meetings were involved with terrorist organizations and the distribution of child pornography. Jin is believed to be in China, and the FBI released a wanted poster. The U.S. government has long warned organizations, including tech companies, that doing business within China carries extra risk. Organizations are required by law to cooperate with the Chinese government.

Read the full article here.

EXPORT CONTROLS: KEY CHALLENGES

Congressional Research Service | January 14, 2021

Congress has authorized the President to control the export of various items for national security, foreign policy, and economic reasons. Separate programs and statutes exist for controlling different types of exports, including nuclear materials and technology, defense articles and services, and dual-use items and technology—items that have both civilian and military uses. Under each program, U.S. government review and licenses of various types are required before export. The Departments of Commerce, State, and Energy administer these programs, in cooperation with input from other relevant agencies. At the same time, Congress also legislates country-specific sanctions that restrict aid, trade, and other transactions to address U.S. policy concerns about weapons proliferation, regional stability, and human rights, some of which are administered by the Treasury Department.

Read the full report here.

A NEW INSTITUTIONAL APPROACH TO RESEARCH SECURITY IN THE UNITED STATES: DEFENDING A DIVERSE R&D ECOSYSTEM

Melissa Flagg and Zachary Arnold | CSET | January 2021

U.S. research security requires trust and collaboration between those conducting R&D and the federal government. Most R&D takes place in the private sector, outside of government authority and control, and researchers are wary of federal government or law enforcement involvement in their work. Despite these challenges, as adversaries work to extract science, technology, data and know-how from the United States, the U.S. government is pursuing an ambitious research security initiative. In order to secure the 78 percent of U.S. R&D funded outside the government, authors Melissa Flagg and Zachary Arnold propose a new, public-private research security clearinghouse, with leadership from academia, business, philanthropy, and government and a presence in the most active R&D hubs across the United States.

Read the full report here.

TAKING THE HELM: A NATIONAL TECHNOLOGY STRATEGY TO MEET THE CHINA CHALLENGE

Martijn Rasser and Megan Lamberth | CNAS | January 13, 2021

The United States faces a challenge like no other in its history: a strategic competition with a highly capable and increasingly resourceful opponent whose worldview and economic and political models are at odds with the interests and values of the world's democratic states. A rising China poses a fundamental challenge to the economic vitality and national security of the United States and its allies and the currency of liberal democratic values around the world. Technology—a key enabler for economic, political, and military power—is front and center in this competition. Technological leadership—how a country invents, innovates, and deploys technologies to compete economically and to secure its interests—will shape the coming years to a remarkable degree. The United States has maintained such leadership for decades. Today, that leadership is at risk. The United States is failing to rise to the occasion—its policies inadequate and disconnected and its response reactive and disjointed. The country needs a new approach to regain the initiative. The stakes are high and the window for action is closing.

Read the full article here.

NCSC CHIEF ON FOREIGN AND DOMESTIC THREATS THE U.S. FACES

NPR | January 14, 2021

NPR's Mary Louise Kelly talks with William Evanina, director of the National Counterintelligence and Security Center, about the recent Russia hack and the riot at the U.S. Capitol.

Listen to the interview here.

WHITE HOUSE ESTABLISHES NATIONAL ARTIFICIAL INTELLIGENCE OFFICE

Maggie Miller | The Hill | January 12, 2021

The White House Office of Science and Technology Policy (OSTP) on Tuesday announced the establishment of a National Artificial Intelligence Initiative Office as part of an effort by the Trump administration to prioritize AI. The office will be in charge of implementing the nation's AI strategy and overseeing and coordinating work on research between the federal government and the private sector. "The National Artificial Intelligence Initiative Office will be integral to the Federal government's AI efforts for many years to come, serving as a central hub for national AI research and policy for the entire U.S. innovation ecosystem," U.S. Chief Technology Officer Michael Kratsios said in a statement provided to The Hill on Tuesday. The office was established as part of the National Artificial Intelligence Initiative Act, which recently became law as part of the annual National Defense Authorization Act (NDAA). The NDAA included sweeping language to boost research into AI, including the creation of a select committee on the subject and codifying into law new AI research institutes announced last year.

Read the full article here.

CHINESE CORONAVIRUS TESTS PUSHED BY US AGENCIES DESPITE SECURITY WARNINGS

Fox Business | January 13, 2021

At least two federal agencies worked to distribute Covid-19 tests from a Chinese genetics company, despite warnings about security risks from U.S. intelligence and security officials, according to interviews and documents obtained by The Wall Street Journal. In the early days of the virus, BGI Group or people trying to distribute its products approached at least 11 states in a sometimes aggressive push to get the products into government-run laboratories or set up entire labs, according to people who received the approaches and documents. BGI, China's leading genetics company, enlisted a foundation tied to a former U.S. president and used a company linked to the United Arab Emirates' top spy to promote its efforts. A prominent New York real-estate lawyer threatened to complain to California's governor if state health officials there didn't use BGI's tests. Some of the company's testing supplies were used in Nevada, according to the head of the state's Covid-19 task force. BGI has tried in the past to get into the U.S. market and has sold testing equipment to U.S. private labs that advertise their work for government clients.

Read the full article here.