



ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

<https://asce.tamus.edu>

# THE OPEN SOURCE MEDIA SUMMARY

**October 12, 2023**

## **NSA AND CISA REVEAL TOP 10 CYBERSECURITY MISCONFIGURATIONS**

*Sergiu Gatlan | Bleeping Computer | October 5, 2023*

The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) revealed today the top ten most common cybersecurity misconfigurations discovered by their red and blue teams in the networks of large organizations. Today's advisory also details what tactics, techniques, and procedures (TTPs) threat actors use to successfully exploit these misconfigurations with various goals, including gaining access to, moving laterally, and targeting sensitive information or systems. The information included in the report was collected by the two agencies' Red and Blue teams during assessments and during incident response activities. "These teams have assessed the security posture of many networks across the Department of Defense (DoD), Federal Civilian Executive Branch (FCEB), state, local, tribal, and territorial (SLTT) governments, and the private sector," the NSA said.

Read the full article [here](#).

## **OPM ANNOUNCES EXPANSION OF 'CONTINUOUS VETTING' SECURITY CLEARANCE PROCESS FOR CURRENT FEDS**

*Erich Wagner | Government Executive | October 4, 2023*

Biden administration officials on Monday announced plans to expand the use of the new "continuous vetting" process for reviewing existing federal workers' background checks to all "public trust" government positions by September 2024. Part of an initiative dating back to the Trump administration, continuous vetting refers to a new process by which the federal government uses automated data checks, such as credit histories and criminal records, to continuously monitor federal workers' suitability to maintain a security clearance or otherwise serve in positions that require public trust. It is designed to replace the existing process, known as periodic reinvestigations, and proponents hope the new process will ease some of the pressure that follow-up investigations place on the security clearance process, particularly the backlog of background checks required for federal job candidates to start work at their new jobs. Additionally, continuous vetting could catch potential red flags earlier, giving agencies a chance to offer support to federal workers experiencing difficulties before the problem can escalate.

Read the full article [here](#).

## **OPED: US PRIVATE SECTOR MUST TEAM WITH GOVERNMENT TO COUNTER CHINA**

*Greg Levesque | Warrior Maven | October 5, 2023*

Are the United States and our allies willing to do what is necessary to effectively counter the People's Republic of China's Military-Civil Fusion Doctrine? The People's Republic of China's expansive ambitions to dominate the global technology sector knows no bounds. Yet – despite a seemingly endless stream of warnings, thefts, and provocations – the U.S. and our allies still have no coherent plan to counter China's bold actions which erase the line between the commercial sphere and geopolitical strategy. To China, commercial conflict and nation-state conflict are not separate; they are part of the same ongoing effort for global dominance. The latest: China announced a few weeks ago that it is restricting the exports of two metals – gallium and germanium – vital for the manufacturing of semiconductors.

Read the full article [here](#).

---

## **NSA AND CISA RED AND BLUE TEAMS SHARE TOP TEN CYBERSECURITY MISCONFIGURATIONS**

*The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) Joint Cybersecurity Advisory | October 2023*

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations. Through NSA and CISA Red and Blue team assessments, as well as through the activities of NSA and CISA Hunt and Incident Response teams, the agencies identified the following 10 most common network misconfigurations:

1. Default configurations of software and applications
2. Improper separation of user/administrator privilege

Read the full article [here](#).

---

## **ESPIONAGE FUELS GLOBAL CYBERATTACKS**

*Tom Burt | Microsoft | October 5, 2023*

In the past year, cyberattacks have touched 120 countries, fueled by government-sponsored spying and with influence operations (IO) also rising. At times, nearly half of these attacks targeted NATO member states, and more than 40% were leveled against government or private-sector organizations involved in building and maintaining critical infrastructure. While headline-grabbing attacks from the past year were often focused on destruction or financial gain with ransomware, data shows the predominant motivation has swung back to a desire to steal information, covertly monitor communication, or to manipulate what people read. For example:

- Russian intelligence agencies have refocused their cyberattacks on espionage activity in support of their war against Ukraine, while continuing destructive cyberattacks in Ukraine and broader espionage efforts

Read the full article [here](#).

## DEPARTMENT OF DEFENSE SEEKS TO COMBAT UNDUE FOREIGN INFLUENCE IN HIGHER EDUCATION INSTITUTIONS WITH FUNDING RESTRICTIONS

Madeleine K. Rodriguez, Shrutih Tewarie and Susanna Chi | *Foley Hoag* | October 3, 2023

DoD recently released a [policy](#) addressing unwanted foreign influence on DoD-funded research. According to the policy, DoD will conduct risk-based security reviews and assess potential conflicts of interest and conflicts of commitment for fundamental research proposals.<sup>[1]</sup> If a security review exposes risks that cannot be mitigated, DoD will not fund the research. Alongside the policy, DoD also [released](#) a list of foreign entities that have been confirmed to engage in malign activities. According to DoD, collaboration with a foreign entity on the list increases the risk of research results being misappropriated to the detriment of U.S. national security. With a new academic year already underway, higher education institutions engaging in fundamental research should carefully note this new development.

Read the full article [here](#).

---

## U.S. FINES STANFORD \$2M FOR FAILING TO DISCLOSE FOREIGN RESEARCH FUNDS

Darryl Coote | *United Press International* | October 3, 2023

Stanford University has agreed to pay nearly \$2 million to resolve allegations that it submitted research proposals to federal agencies, including the military, without disclosing that faculty members were receiving funding from foreign sources, including China. The \$1.9 million settlement dated Thursday but announced by the Justice Department on Monday only resolves allegations and does not determine liability, federal prosecutors said. "Protecting research and development programs funded by taxpayer dollars is a top priority for us," Acting Assistant Inspector General for Investigations Michael Graham of the NASA Office of Inspector General said in a statement. "The settlement agreement with Stanford University is the result of a joint effort to guard against fraud, waste and abuse in government grants." A Stanford University spokesperson told UPI in a statement that it is "pleased" this issue has been resolved and that it is committed to ensuring its researchers meet federal compliance responsibilities.

Read the full article [here](#).

---

## RESEARCH INTEGRITY AND SECURITY: EXPLORING FUNDING AGENCY ROLES IN SUPPORTING RESPONSIBLE INTERNATIONALIZATION AND RECIPROCITY

Tommy Shih | *Insight Paper* | 2023

Since the end of the 1990s and in the wake of the Cold War, research publication volume has significantly increased globally and scientific progress has been rapid. Not only have advancements and growth come from Western countries, but also from other parts of the world such as Asia, and China in particular (Miao et al., 2022). In Latin America and the Middle East scientific development is also clearly evident. While these developments are positive, and stem from increased collaboration and brain circulation in the world, they have also led to changing global power balances (Marginson, 2022). In light of a multipolar power dynamic, some governments have become progressively apprehensive of the logic of openness under which researchers and universities work (Nature, 2021). Some of these concerns include:

Read the full article [here](#).

## CHIPS AND SCIENCE IMPLEMENTATION AND OVERSIGHT

Sethuraman Panchanathan | Testimony before the Senate Committee on Commerce, Science and Technology | October 4, 2023

Chair Cantwell, Ranking Member Cruz, and Members of the Committee, it is a privilege to appear before you today to discuss the National Science Foundation's implementation of the CHIPS and Science Act of 2022, and how the agency is building upon decades of successful investments in science, engineering, and technology to ensure that the United States remains the global leader in innovation into the future. Established by the National Science Foundation Act of 1950 (P.L. 81-507), the National Science Foundation (NSF) is an independent federal agency charged with the mission "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes."

Read the full article [here](#).

---

## PRODUCT SERIALISATION – A TOOL TO HELP COUNTER DIVERSION AND ILLICIT TRADE

Paul Curwell | ForewarnedBlog.Com | October 8, 2023

When was the last time you bought diverted product? Illicit Trade and diversion is a problem which keeps growing. Have you ever purchased a counterfeit product? Would you know if you did? If you're a regular online shopper the chances are good that you've come across illicit product, possibly without knowing it. I was recently at my local barbers getting a haircut when I noticed the container of a popular brand of talcum powder. Only the logo and product name was in English – everything else was in Indonesian. My barber mentioned he hadn't noticed, but bought it because it was being sold cheaply online. This is an example of product diversion.

Read the full article [here](#).

---

## US, UK UNIVERSITIES LEAD 'THE' RANKINGS BUT CHINA RISING

University World News | September 27, 2023

The top of the latest Times Higher Education or THE World University Rankings, released on Wednesday 27 September, remains dominated by institutions in the United States and United Kingdom, with the University of Oxford from the UK taking top spot for an unprecedented eight consecutive years. But the upward march of Chinese universities continues. The's World University Rankings 2024 assess research-intensive universities across 18 calibrated performance indicators covering their core missions of teaching, research, knowledge transfer and internationalisation. In the 20th year of the ranking 1,904 universities – up from 1,799 last year – from 108 countries and regions are ranked.

Read the full article [here](#).

---

## THE TEXAS A&M UNIVERSITY SYSTEM

*The Academic Security and Counter Exploitation  
Program is coordinated by The Texas A&M  
University System Research Security Office as a  
service to the academic community.*

<https://rso.tamus.edu>



# USEFUL RESOURCES

## DSS Cyber Insider Threat

YouTube

The technological revolution has changed everything about our lives: how we conduct business, travel, bank, date, and even how we spy. The Cyber Insider Threat Course explores the manifestation of traditional espionage indicators in a cyber-environment, identifies new indicators specifically related to the IT insider threat, and discusses observable and reportable behaviors that help to detect, deter, and neutralize cyber insider threat.

View the full resource [here](#).

---

## CYBERSECURITY AWARENESS MONTH

*Cybersecurity & Infrastructure Security Agency*

Since 2004, the President of the United States and Congress have declared the month of October to be Cybersecurity Awareness Month, a dedicated month for the public and private sectors to work together to raise awareness about the importance of cybersecurity. This is the 20th Cybersecurity Awareness Month and it has grown into a collaborative effort between government and industry to enhance cybersecurity awareness, encourage actions by the public to reduce online risk and generated discussion on cyber threats on a national and global scale.

View the full resource [here](#).

---

## SAFEGUARDING INTERNATIONAL SCIENCE

*Gregory F. Strouse, Timothy Wood, Claire Saundry, Philip Bennett, and Mary Bedner  
National Institutes of Standards and Technology (NIST) | August 2023*

The U.S. research ecosystem retains its leadership by actively engaging with the global community through the conduct of mutually beneficial joint research and the welcoming of international scientists. Coupled with that, the national and economic security of the United States depends on effective risk management practices for organizations that engage in international research collaborations. Establishing a Safeguarding International Science Research Security Program ("Program") through an implemented framework provides checks and safeguards at key steps in program development and implementation to help manage responsible international engagement.

View the full resource [here](#).

---

## THE TEXAS A&M UNIVERSITY SYSTEM

*The Academic Security and Counter Exploitation  
Program is coordinated by The Texas A&M  
University System Research Security Office as a  
service to the academic community.  
<https://rso.tamus.edu>*