TOM COTTON
ARKANSAS

326 Russell Senate Office Building
Washington, DC 20510
Phone: (202) 224–2353

United States Senate

COMMITTEES
SELECT COMMITTEE ON INTELLIGENCE
CHAIRMAN
SENATE ARMED SERVICES COMMITTEE
JOINT ECONOMIC COMMITTEE
ENERGY AND NATURAL RESOURCES

December 17, 2025

The Honorable Sean Cairncross
Director
Office of the National Cyber Director
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Mr. Cairncross,

I write concerning a critical national security risk of foreign adversaries, particularly China and Russia, contributing to the open source software (OSS) ecosystem that underpins American software systems, including Department of War software. OSS relies on a trust-based, global community of contributors to ensure that software stays accessible, secure, and updated. Historically, such a framework has pulled in talent from around the world to build projects that have become ubiquitous, foundational technology. Unfortunately, there are reports that state-sponsored software developers and cyber espionage groups have started to exploit this communal environment, which assumes that contributors are benevolent, to insert malicious code into widely used open source codebases.

For example, last year, an intentionally planted backdoor was discovered in XZ Utils, a critical open source tool.[1] The actor behind this malicious code, known as “Jia Tan”, spent years building credibility and lying in wait until the right moment. A Russia-based developer is the sole maintainer of fast-glob, another piece of OSS embedded in numerous software packages in the Department of War, raising alarms about potential compromises.[2] Chinese giants like Alibaba and Huawei are ranked in the top 20 contributors worldwide in the most recent Open Source Contributor Index.[3] As you know, the Chinese Communist Party’s (CCP) national security laws impose broad obligations on China-based entities, including compelling companies to provide technical assistance to further CCP goals.[4]

OSS is the backbone of U.S. government systems, including mission-critical defense systems, where we reap the numerous benefits of OSS to innovate, develop, and deploy technology quickly. However, leaving our reliance on OSS unmonitored is exposing America to increasingly dangerous risks. Secretary Hegseth has already sounded the alarm, releasing a memorandum declaring that the Department of War “will not procure any…software susceptible to adversarial foreign influence…and must prevent such adversaries from introducing malicious capabilities into the products and services utilized by the Department.”[5] He also directed the Department to purge its software of Chinese involvement.[6]

[1] https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/

[2] https://www.nextgov.com/cybersecurity/2025/08/report-russia-based-yandex-employee-oversees-open-source-software-approved-dod-use/407703/

[3] https://opensourceindex.io

[4] https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

[5] https://media.defense.gov/2025/Jul/22/2003759081/-1/-1/1/ENHANCING-SECURITY-PROTOCOLS-FOR-THE-DEPARTMENT-OF-DEFENSE.PDF

[6] https://www.war.gov/News/News-Stories/Article/Article/4288992/pentagon-halts-chinese-coders-affecting-dod-cloud-systems/

As the Office of the National Cyber Director holds responsibility for coordinating implementation of national cyber policy and government-wide cybersecurity, you are well-positioned to lead the U.S. government in addressing this cross-cutting vulnerability. I respectfully request that you take steps to build up the federal government's capability to maintain awareness of provenance and foreign influence on OSS and track contributions from developers in adversary nations.

Thank you for your attention to this matter.

Sincerely,

Tom Cotton

Tom Cotton
United States Senator