

JOHN MOOLENAAR, MICHIGAN  
CHAIRMAN  
ROB WITTMAN, VIRGINIA  
ANDY BARR, KENTUCKY  
DAN NEWHOUSE, WASHINGTON  
DARIN LAHOOD, ILLINOIS  
NEAL DUNN, FLORIDA  
DUSTY JOHNSON, SOUTH DAKOTA  
ASHLEY HINSON, IOWA  
CARLOS GIMENEZ, FLORIDA  
GUS BILIRAKIS, FLORIDA  
YOUNG KIM, CALIFORNIA  
NATHANIEL MORAN, TEXAS  
ZACH NUNN, IOWA

RAJA KRISHNAMOORTHY, ILLINOIS  
RANKING MEMBER  
KATHY CASTOR, FLORIDA  
ANDRÉ CARSON, INDIANA  
SETH MOULTON, MASSACHUSETTS  
RO KHANNA, CALIFORNIA  
HALEY STEVENS, MICHIGAN  
RITCHIE TORRES, NEW YORK  
SHONTEL BROWN, OHIO  
GREG STANTON, ARIZONA  
JILL TOKUDA, HAWAII



Congress of the United States  
House of Representatives  
SELECT COMMITTEE ON CHINA

January 15, 2026

Interim Director Mr. Brian Stone  
National Science Foundation  
2415 Eisenhower Ave  
Alexandria, VA 22314

Dear Interim Director Stone:

I write to urge the National Science Foundation (NSF) immediately revoke access for all Chinese entities to the NSF's Advanced Cyberinfrastructure Coordination Ecosystem: Services & Support (ACCESS) program. Specifically, entities affiliated with the People's Republic of China (PRC)—including institutions designated on U.S. government restricted entity lists—have obtained approved access and login credentials via ACCESS to U.S.-funded high-performance computing infrastructure. Some of the high-performance computing infrastructure utilize graphics processing units (GPUs) that are export controlled. Given the strategic importance of advanced compute resources for artificial intelligence, modeling and simulation, and other dual-use technologies, these findings warrant a review of ACCESS eligibility, credentialing, and oversight mechanisms to ensure protection of U.S. national security interests.

ACCESS is a national research cyberinfrastructure ecosystem that supports computational- and data-intensive research. It plays a critical role in sustaining U.S. leadership in science and technology, strengthening economic competitiveness, and advancing national security interests.<sup>1</sup> It helps researchers and educators utilize the nation's advanced computing systems and services such as supercomputing applications, artificial intelligence, machine learning, big data analysis and storage.<sup>2</sup> ACCESS was funded through a five-year, \$52 million NSF award.<sup>3</sup>

Eligibility for ACCESS requires the user to be a U.S.-based researcher or educator. However, international researchers who are not located in the United States may still obtain access through a U.S.-based researcher who serves as the principal investigator (PI) on the ACCESS request and allocation. An eligible PI may share their allocation by adding collaborators' user accounts to the project. These collaborators may include graduate or undergraduate students, as well as

---

<sup>1</sup> Website, National Science Foundation, About ACCESS, <https://access-ci.org/about/>

<sup>2</sup> *ibid*

<sup>3</sup> *ibid*

colleagues based outside of the United States. Additionally, there are multiple ways to obtain an account and login credentials for ACCESS.<sup>4,5</sup>

The Select Committee conducted an open-source review of entities that have registered for and received approved accounts and login credentials under ACCESS. This review identified numerous Chinese institutions that appear on current U.S. government restricted entity lists. Identified entities include the People’s Liberation Army’s National University of Defense Technology; all of the “Seven Sons of National Defense” (国防七子) universities; and multiple institutions co-administered by the State Administration for Science, Technology, and Industry for National Defense (SASTIND, 国家国防科技工业局), including the University of Science and Technology of China.<sup>6</sup>

Figure 1 – NSF ACCESS Login Page Outlining Approved Identity Accounts for Login Access

The screenshot shows the NSF ACCESS login interface. At the top left is the ACCESS logo. Below it is a section titled "Consent to Attribute Release" with a dropdown arrow. The text reads: "ACCESS Allocations requests access to the following information. If you do not approve this request, do not proceed." Below this is a bulleted list of requested information: "Your CILogon user identifier", "Your name", "Your email address", and "Your username and affiliation from your identity provider".

Below the consent section is a "Select an Identity Provider" section. It features a dropdown menu with "National University of Defense and Technology" selected. There is a "Remember this selection" checkbox with a question mark icon. A yellow "LOG ON" button is centered below the dropdown. At the bottom left, a small text line states: "By logging on to this site, you agree to the [privacy policy](#)."

ACCESS provides researchers with access to some of the United States’ most advanced federally supported high-performance computing resources, including systems operated by the Pittsburgh

<sup>4</sup> One way is to go through ACCESS registration and provide petitioner attributes which will then go through the process of “Use Policy” acceptance, finalization, and notification.

<sup>5</sup> Website, National Science Foundation, ACCESS Registration, [https://registry.access-ci.org/registry/co\\_petitions/petitionerAttributes/447048/token:138a2983a527731b960f8e2068d2f2dc1fd5d055](https://registry.access-ci.org/registry/co_petitions/petitionerAttributes/447048/token:138a2983a527731b960f8e2068d2f2dc1fd5d055)

<sup>6</sup> Website, National Science Foundation, ACCESS CILogon username affiliation identity provider, [https://cilogon.org/authorize?client\\_id=cilogon%3A%2Fclient\\_id%2F2be055700cdcb8393fe843843c563141&nonce=0072dae1f21646ae929c06feb69d2d3a&redirect\\_uri=https%3A%2F%2Fallocations.access-ci.org%2Flogin%2Fcilogon%2Fcallback&response\\_type=code&scope=openid%20email%20profile%20org.cilogon.userinfo&state=83d91e6c03810c0a5f8ca7c77a21a888](https://cilogon.org/authorize?client_id=cilogon%3A%2Fclient_id%2F2be055700cdcb8393fe843843c563141&nonce=0072dae1f21646ae929c06feb69d2d3a&redirect_uri=https%3A%2F%2Fallocations.access-ci.org%2Flogin%2Fcilogon%2Fcallback&response_type=code&scope=openid%20email%20profile%20org.cilogon.userinfo&state=83d91e6c03810c0a5f8ca7c77a21a888)

Supercomputing Center, the Texas Advanced Computing Center, Texas A&M University, and other major national providers. These facilities host cutting-edge computational infrastructure critical to advanced research in artificial intelligence, modeling and simulation, and other dual-use technology areas.<sup>7</sup> According to ACCESS operational documentation for Texas A&M University's Accelerating Computing for Emerging Sciences (ACES) system, the ACES cluster includes advanced GPUs, including NVIDIA H100s.<sup>8</sup> The NVIDIA H100 is subject to U.S. export controls and requires a license for export to certain foreign countries, including the PRC.<sup>9</sup>

In light of these findings, the Select Committee has concerns that ACCESS may be enabling Chinese entities, including previously blacklisted entities, to circumvent the U.S. export-control regime. By accessing U.S.-based high-performance computing resources remotely, these entities may be able to conduct advanced simulations, data processing, and model training from within China without ever having to obtain export-controlled GPUs or licenses and at the expense and time of U.S. research timelines. This raises fundamental questions about whether current ACCESS eligibility, allocation, and oversight mechanisms adequately account for national security risks, deemed export risks, and align with the intent of U.S. export controls. Additionally, these findings raise questions as to why institutions affiliated with the PLA and China's defense research establishment are being issued approved login credentials that allow them to apply for compute time and access U.S.-funded supercomputing infrastructure. Regardless of any partnership with a U.S.-based PI, Chinese entities, particularly blacklisted ones, should not be granted access to advanced U.S.-funded computing infrastructure through the NSF ACCESS program.

I respectfully request that NSF immediately review all PRC-based entities that have been approved to have login credentials for the NSF ACCESS program. NSF, at a minimum, should immediately revoke all login credentials and access to ACCESS—and the associated high-performance computing resources—for any entity currently designated on a U.S. government restricted or national security–related entity list.

Additionally, I request the following information by February 6, 2026.

1. Please provide a record of all Chinese entities that have been issued approved login credentials under the NSF ACCESS program.
2. Please provide a list of Chinese entities that have been approved to access compute resources through the NSF ACCESS program, including the specific projects, allocations, and resource providers associated with each approval.
3. Has any Chinese entity or individual been granted access to U.S. supercomputing infrastructure through the NSF ACCESS program during a period in which a U.S.-based entity or individual was awaiting approval or allocation of compute time?

---

<sup>7</sup> Website, National Science Foundation, Resource Providers, <https://access-ci.org/about/resource-providers/>

<sup>8</sup> Website, National Science Foundation, ACCESS Active Resources, <https://operations.access-ci.org/resources/access-allocated>

<sup>9</sup> Publication, Hannah Dohmen and Jacob Feldgoise, Center for Security and Emerging Technology, A Bigger Yard, A Higher Fence: Understanding BIS's Expanded Controls on Advanced Computing Exports, December 4, 2023, <https://cset.georgetown.edu/article/bis-2023-update-explainer/>

Interim Director Stone

January 15, 2026

Page 4 of 4

The Committee stands ready to work with NSF to ensure that U.S.-funded high-performance computing infrastructure—built to advance American scientific leadership and economic competitiveness—is not exploited by foreign adversaries to accelerate their technological or military capabilities. Safeguarding access to advanced compute resources is essential to protecting the integrity of the U.S. research enterprise and securing it against foreign threats.

Thank you in advance for your prompt attention to this matter.

Sincerely,



---

John Moolenaar

Chairman