Trust. Verified.

AMERICAN SECURITY FUND

GeoComply

The Chip Security Act

Leveraging Existing Location Verification Technology to Adapt Export Controls to the Artificial Intelligence (AI) Age

February 2026

To lead the AI age, the United States must evolve its export control framework from trusting that semiconductor exports go where they should to **verifying** that they do. Congress should pass the **Chip Security Act** and make **location verification** a core element of the United States' strategic controls.

Semiconductors, or "chips," are the most strategic and economically important technology in the modern world. They power all leading AI applications—from early disease detection and material science innovation to information operations and autonomous weapons systems. Their unparalleled importance is reflected in both the valuations of the companies that make them and the lengths countries go to obtain them.

As the primary innovator of advanced chips, the United States has critical leverage over the AI supply chain. To maintain our leverage (and prevent China and other competitors from weaponizing AI models), the United States put strict export controls on chips and associated equipment.

While the controls have impacted China's compute capabilities, major loopholes have emerged. Even though chip manufacturers conduct due diligence on overseas clients pre-export, there is little they can do to monitor chips' locations after they leave their factories. Additionally, the Department of Commerce's Bureau of Industry and Security (BIS)—the primary U.S. Government body responsible for overseeing U.S. export controls—is chronically understaffed and under-resourced, which complicates the monitoring of global data centers and deployed servers.

If we wish to lead the AI age, we must not let our export controls atrophy; we must know where our advanced chips go.

THE PROBLEM: EXPORT CONTROL DIVERSION

America's export control regime is premised on trust, not on verification—and is being exploited by third countries, shell companies, and smuggling networks.

The Center for a New American Security (CNAS) estimates that up to 30% of China's AI inference and up to 40% of its AI training capabilities are reliant on advanced chips that were illicitly smuggled into the country.[1]

Several Department of Justice (DOJ) actions in the second half of 2025 exposed the existence of sophisticated chip smuggling networks. In August, the DOJ charged two Chinese nationals with conspiring to export tens of millions of dollars' worth of sensitive chips to China without required licenses.[2] In November, the DOJ unsealed an indictment against two U.S. citizens and two Chinese nationals, accusing them of conspiring to export thousands of NVIDIA's advanced Graphics Processing Units (GPUs) to China through transshipment points in Malaysia and Thailand.[3] And in December, the DOJ arrested two businessmen and charged them with conspiracy to smuggle export-controlled AI hardware to China through a network of "straw purchasers."[4]

The bottom line is that while federal law enforcement has devoted considerable resources to export enforcement, chips are still slipping through the cracks. According to The Information, DeepSeek—the Chinese AI lab whose R-1 Model disrupted the AI industry in January 2025—has used "thousands" of NVIDIA's export-restricted Blackwell chips to power its models. Specifically, DeepSeek has "tapped chips that were installed in data centers in unspecified countries, then dismantled and shipped to China after clearing inspection by companies developing server equipment."[5] While the true scale of export diversion is unknown, the credible allegations that DeepSeek has stolen thousands of U.S.-made chips to train and develop its models to stay at the cutting edge of AI demonstrate that export controls are necessary, but export compliance is being inadequately verified.

[1] Grunewald, Erich, and Tim Fist. "Countering AI Chip Smuggling Has Become a National Security Priority: An Updated Playbook for Preventing AI Chip Smuggling to the PRC." Center for a New American Security, June 11, 2025.
[2] U.S. Attorney's Office, Central District of California. "Two Chinese Nationals Arrested on Federal Complaint Alleging They Illegally Shipped to China Sensitive Microchips Used in AI Applications." Press release, August 5, 2025.
[3] Office of Public Affairs. "U.S. Citizens and Chinese Nationals Arrested for Exporting Artificial Intelligence Technology to China." U.S. Department of Justice. Press release, November 20, 2025.
[4] Office of Public Affairs. "U.S. Authorities Shut Down Major China-Linked AI Tech Smuggling Network." U.S. Department of Justice. Press release, December 8, 2025.
[5] Yang, Jing. "DeepSeek Using Banned Nvidia Chips in Race to Build Next Model." *The Information*, December 10, 2025.

THE SOLUTION: LOCATION VERIFICATION

Smugglers consistently employ the same tactic: claiming that chips are destined for permitted jurisdictions—often countries in Southeast Asia—and then reshipping them from those locations to China. In doing so, they are depending on chip exporters to lack the technical ability to cross-check the purported export destinations of chips with their true physical locations.

Thankfully, Congress has taken the initiative to advance the technical capabilities that can stop this circumvention. The Chip Security Act—which, at the time of the publication of this report, has 9 Senate and 33 House sponsors—would "require the Secretary of Commerce to issue standards with respect to chip security mechanisms for integrated circuit products."[9] While chip exporters would have several options for "chip security mechanisms," including periodic physical inspections, location verification would likely be the primary monitoring technique.

The principles of location verification are simple: devices with the capability to connect to global internet or telecommunications networks can access signals that can be employed to deduce their location. While techniques like satellite positioning (GPS) can geolocate personal devices—such as laptops, tablets, and mobile phones—AI chips require an alternative approach: **latency-based (or "ping-based") location verification.**

PUTTING POLICY INTO PRACTICE: THE MECHANICS OF LATENCY-BASED LOCATION VERIFICATION

Latency-based location verification relies on two primary technologies: chip identity verification and "Ground Truth" servers.

THE EVOLVING SCOPE OF EXPORT CONTROLS

In recent months, the export control landscape has been upended by the administration's decision to send NVIDIA H200s and comparable classes of chips to certain licensed entities in the People's Republic of China (PRC).[6] While this disrupts the status quo, it does not invalidate the need for robust location verification.

First, considerable chip controls remain in effect. Not only are H200 sales prohibited to many sectors in the PRC—such as state-owned enterprises (SOEs) and military end users—but many more advanced chips, such as NVIDIA's Blackwell GPU (allegedly being used to train DeepSeek models) and forthcoming Rubin GPU, remain completely embargoed. As the world increasingly adopts more advanced chips, these devices will become the focus of smuggling networks and export enforcement officials, alike.

Second, proposed legislation in Congress suggests that the scope of export controls could expand in the coming months. The AI OVERWATCH Act, which would give Congress the ability to directly review, and potentially deny, chip sales to "countries of concern", recently advanced out of the House Foreign Affairs Committee (HFAC) with overwhelming bipartisan support.[7] [8]

If Chinese AI labs make further model advances using U.S. chip architecture—a significant possibility—Congressional desire to strengthen export controls will intensify, which will, in turn, bolster the need for location verification.

To verify its identity, as part of its core architecture**,** an advanced chip uses a hardware-isolated Root of Trust containing a unique, unextractable, private key, which cryptographically signs a challenge request, creating a digital signature that can be validated (but cannot be forged). The process ensures the device is a genuine advanced chip rather than a software spoof, establishing a trusted endpoint to enable subsequent location verification.

A validated signature enables an advanced chip to securely connect with a network of Ground Truth servers—specially designated infrastructure controlled by trusted entities and hosted in friendly jurisdictions—which send "pings" over internet infrastructure to the chip and measure the time it takes for data to travel to the device and back (Round Trip Time or "RTT").

Because internet signals travel at predictable speeds, RTT between two devices is convertible into an approximate physical distance. And while a measurement taken from a single server will only provide a linear distance, latency measurements derived from multiple server locations allow for multilateration: a process in which server pings produce a circle encompassing the maximum geographic area in which a chip could possibly be located. As additional servers are added to the system, the possible location of a chip reduces to the area in which the circles intersect. The more servers added, the more overlapping circles reduce the possible chip location range (see Figure 1).

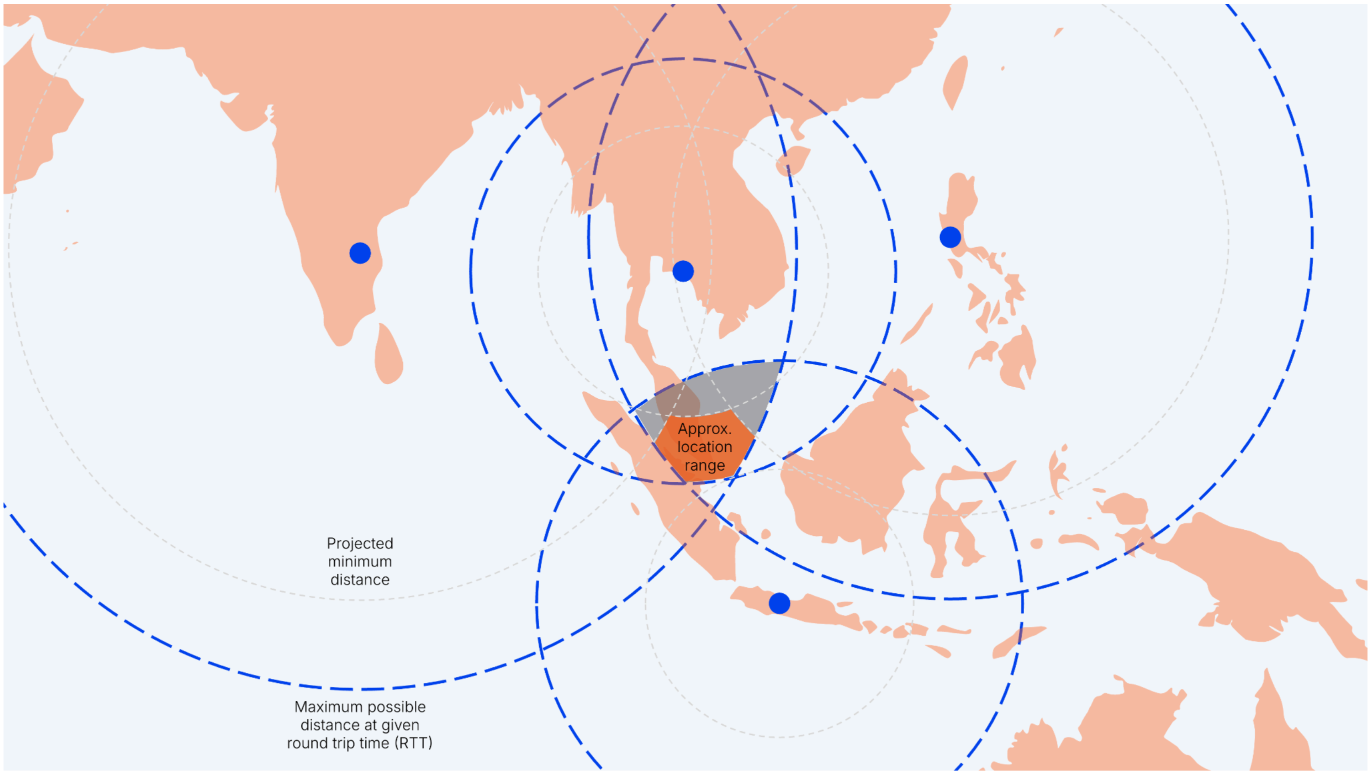
[6] Bureau of Industry and Security. "Department of Commerce Revises License Review Policy for Semiconductors Exported to China." U.S. Department of Commerce. Press release, January 13, 2026.

[7] Freifeld, Karen. "US House Panel to Vote on Bill to Give Congress Authority over AI Chip Exports." Reuters, January 21, 2026..

[8] U.S. House Foreign Affairs Committee. "Chairman Mast, HFAC, advances AI Overwatch Act." Press release, January 21, 2026.

[9] U.S. Congress. House. *Chip Security Act*. HR 3447. 119th Cong., 1st sess. Introduced in House May 15, 2025..

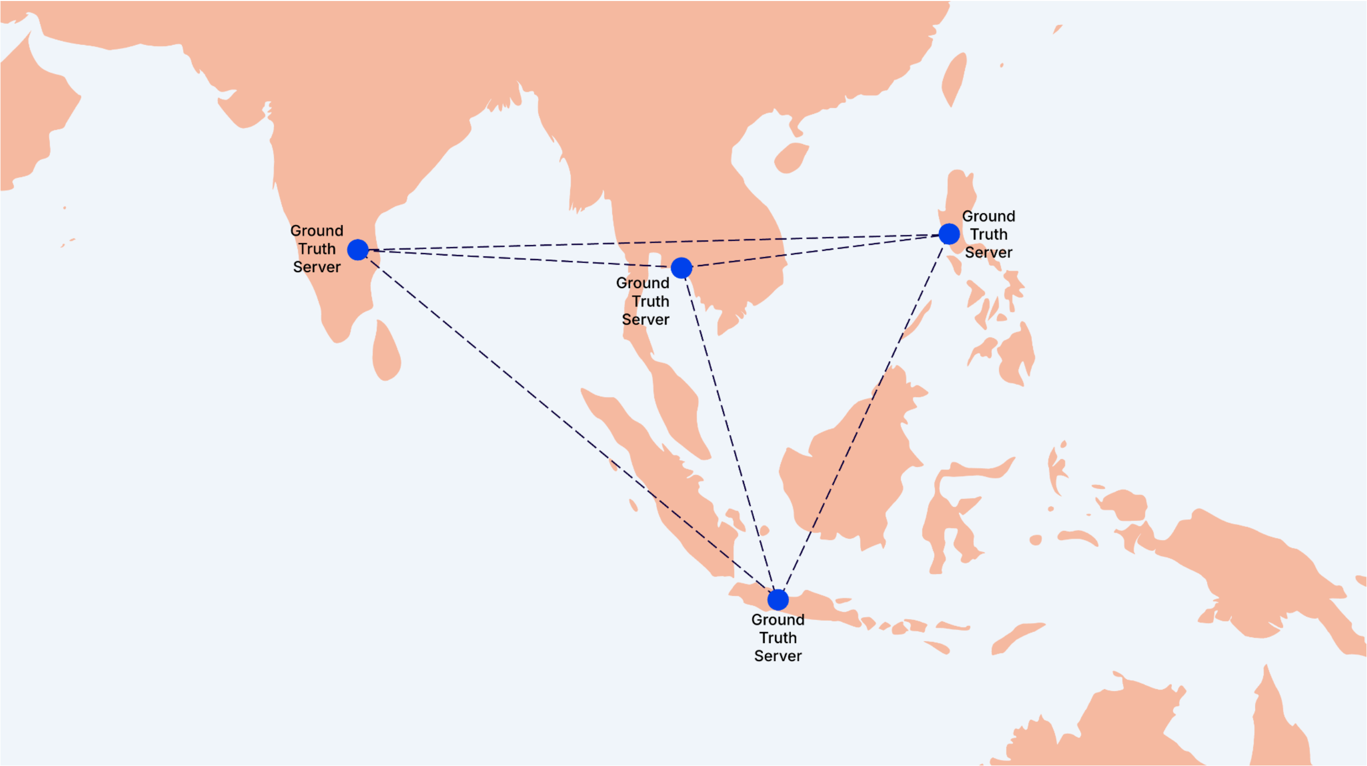
Figure 1: Multilateration in Practice



Note: Graphic simplifies system complexity for visualization purposes

Ensuring that the ground truth servers—and, by extension, the entire verification network—remain secure requires regular validation of the servers' locations. Simultaneous pings between fixed servers enable mutual validation of each individual server, preventing bad actors from compromising any single point in the network (see Figure 2).

Figure 2: Network Validation Through Server-to-Server Communications



Note: Graphic simplifies system complexity for visualization purposes

Of course, a primary concern for all export control mechanisms is the risk of evasion through location spoofing—often conducted by routing a signal through a remote server in close proximity to a chip's original intended destination. However, latency-based verification is uniquely resilient. While a bad actor can use various methods to artificially add latency—making a chip appear further away than it is—it is physically impossible to make a chip appear closer to a server than it is. Illustratively, this constraint ("maximum speed of data") would see a ping between a chip legitimately residing in Malaysia and a Ground Truth Server in Singapore have a relatively short RTT, which would be physically impossible to spoof if the chip was illicitly diverted to a country of concern further from the Ground Truth Server.

Compared to more straightforward means of geolocation like GPS, latency-based location verification has physical complexities that make it technically challenging. First, data does not always travel in straight lines, but on paths dictated by geography. If an internet cable has to go around a mountain or an undersea obstacle, its "distance" will look longer than it is. Second, if an internet network experiences congestion, a data packet may be delayed for a few milliseconds, making it look further away than it is. And finally, a data packet may encounter additional hurdles as it navigates data center infrastructure.

While such considerations may limit basic latency-based measurement systems, a well-designed system will possess characteristics that enhance accuracy, detect complex spoofing techniques, and produce robust intelligence on diverted chips, rendering it a powerful—and non-intrusive—tool for preventing unauthorized chip diversion.

THE OFAC PRECEDENT: LOCATION VERIFICATION AS PART OF NATIONAL SECURITY REGULATION

The Treasury Department's Office of Foreign Assets Control (OFAC), BIS's financial sanctions counterpart, requires companies providing online financial services, from banking to cryptocurrency trading, to know their users' locations to ensure their platforms do not provide restricted services to individuals residing in comprehensively sanctioned jurisdictions.

OFAC specifically recommends the use of "geolocation data" to facilitate compliance.[10] In the last 5 years, OFAC, along with the DOJ and Financial Crimes Enforcement Network (FinCEN), has issued billions of dollars in fines to financial institutions for providing services to individuals physically located in comprehensively sanctioned jurisdictions.[11]

If location verification technology can support national security priorities with respect to financial services, then the same concept can support the same goals with respect to advanced chips.

CONCLUSION

The fate of global AI leadership hinges on effective compute governance. The United States must meet the moment by strengthening its export controls. There are many compelling proposals about what the scope of those export controls should be, but these proposals will only be effective if accompanied by robust verification mechanisms**.** Cutting-edge location verification—as envisioned in the **Chip Security Act**—can effectively track the chips. The result will be American prosperity through secure exports, trade, and diffusion of U.S. made technology.

American Security Fund (501)(c)(4)) is a nonprofit nonpartisan organization advancing American tech superiority by connecting industry, government, and ethics. Read more at www.americansecurityfund.com.

GeoComply is a cybersecurity company specializing in location and device analytics. It operates in highly regulated sectors, and its technology is embedded on 200+ million devices worldwide. Read more at geocomply.com.

[10] Office of Foreign Assets Control. "Sanctions Compliance Guidance for the Virtual Currency Industry." U.S. Department of the Treasury. October 15, 2021. https://ofac.treasury.gov/media/913571/download?inline.

[11] Stringham, Christopher. "FCC Essential N.4 - The Critical Role of Location in Sanctions Screening." Neterium (blog). Accessed January 26, 2026. https://www.neterium.io/insights/fccessentials/fcc-essential-n-4-the-critical-role-of-location-in-sanctions-screening-/.