COMPREHENSIVE LIST OF THE COMMISSION'S 2026 RECOMMENDATIONS

Part II: China's Efforts to Expand Its Global Power and Influence

Chapter 3: China's Other Front: India and the Future of U.S. Strategy in the Indo-Pacific

1. The Federal Government has spent years building a wall against risky suppliers in strategic sectors. It now needs a purchasing strategy that makes trusted pharmaceutical production commercially viable. The central obstacle is commercial: manufacturers cannot justify investing in alternative sources of active pharmaceutical ingredients (APIs) and key starting materials (KSMs) without confidence that buyers will continue purchasing from them even when cheaper Chinese supply is available.

   To break China's leverage over the supply of essential medicines, Congress should establish a Comprehensive Critical Drug Diversification (C2D2) program built around U.S.-India cooperation. The program should:

   - Establish a pharmaceutical supply chain early warning mechanism for a list of essential medicines to identify APIs, KSMs, and critical intermediates and their production sites; identify single-country and single-facility dependencies; flag emerging disruptions; and direct purchasing and investment toward gaps.
   - Authorize the U.S. Department of Health and Human Services to establish a Federal Trusted Demand Program, including multiyear commitments for essential medicines made with qualifying U.S. or trusted partner APIs and KSMs. The U.S. government should buy finished medicines it needs while making verified sourcing of critical inputs a condition for participation. The U.S. government should also ensure consistent purchase pricing across agencies. The program should:
     - Coordinate how participating agencies verify suppliers and the origins of their critical inputs, including subpoena authority to demand documentation;
     - Have the ability to make multi-year purchase commitments for essential medicines; and
     - Direct the U.S. government to work with providers to address cost disparities of buying medicines under long-term contracts.

- Include an initiative to support public and private investment in API and KSM production in India. For APIs, producers should be mandated to prove minimal and declining reliance on Chinese KSMs to receive the funding. The initiative should, to the maximum extent practicable, require matching funds from India and coordination with Indian producers to withstand predatory Chinese pricing.

2. As the 14th Dalai Lama advances in age, China is preparing to turn his succession into an international contest over legitimacy and will likely use coercive tools to shape its outcome. India, which hosts the Dalai Lama and the Tibetan government-in-exile and shares a longstanding disputed border with China, is the center of gravity in this dispute.

   Congress should make it the policy of the United States that the Gaden Phodrang Trust is the sole legitimate authority to identify and recognize the successor to the 14th Dalai Lama and that the United States will not recognize any successor selected or installed by the Government of the People's Republic of China. To carry out this policy and ensure U.S. government readiness for the Dalai Lama's succession, Congress should direct the Secretary of State to:

   - Lead an internal interagency tabletop exercise on succession scenarios, with participation by the National Security Advisor, the Director of National Intelligence, and the Secretary of Defense, and brief the appropriate congressional committees on its findings within 180 days.
   - Establish a senior-level channel with the Government of India for succession contingency planning, including intelligence sharing on Chinese influence operations, and report to the appropriate congressional committees on its status within 180 days.
   - Conduct Track 1.5 and Track 2 dialogues and tabletop exercises with Indian counterparts on the political and security implications of succession scenarios.
   - Coordinate with allies and partners on a diplomatic response that denies international legitimacy to any successor selected by the People's Republic of China.
   - Counter succession-related influence operations by strengthening the Central Tibetan Administration's cybersecurity and resilience against China's cyber and artificial intelligence (AI)-enabled disinformation campaigns.

   Congress should provide authorizations and appropriations to carry out these activities.

3. China's efforts to constrain India's regional influence and expand its military presence in the Indian Ocean underscore the importance of a stronger U.S.-India strategic partnership. The United States should deepen operational defense cooperation and foster lasting relationships among the next generation of American and Indian leaders.

Congress should:

- Direct the Secretary of Defense and Chairman of the Joint Chiefs of Staff to engage with their Government of India counterparts to strengthen coordination on undersea and maritime domain awareness in the Indian Ocean.
  - These efforts should prioritize moving beyond military exercises toward sustained operational cooperation, including systematic intelligence and surveillance information sharing, coordinated monitoring of Chinese naval and submarine activity, and improved procedures for responding to maritime threats.
- Create an Indo-American Strategic Leadership Exchange Program to forge generational ties among rising leaders in defense, government, business, and academia.

Chapter 4: China's Predatory Diplomacy in Latin America: Broken Promises, Harmful Practices

4. To enhance the capacity of Latin American countries to screen investments for economic and national security risks, Congress should:
   - Direct the Secretary of the Treasury, in coordination with other members of the Committee on Foreign Investment in the United States (CFIUS), to establish a Foreign Investment Rapid Screening Team (FIRST) that trains and embeds in partner governments in Latin America. FIRST assistance should include:
     - Sending delegations to Latin America to develop screening mechanisms for investment and infrastructure projects as well as to train and work alongside procurement officers, auditors, and investment authorities on anticorruption, contract law, and corporate control structures;
     - Extending technical assistance to subnational governments, which often negotiate major investment and infrastructure projects but have limited capacity to assess national security implications;
     - Coordinating with the U.S. International Development Finance Corporation, Export-Import Bank of the United States, Millennium Challenge Corporation, and U.S. Trade and Development Agency to employ investment and technical assistance resources to incentivize partner countries in Latin America to develop investment screening mechanisms and mobilize U.S. and trusted capital as alternatives to untrusted investors;
     - Coordinating with the Secretary of State and organizations such as the National Endowment for Democracy to utilize their core institutes to strengthen the capacity of government and non-governmental organizations to support investment screening and related good governance initiatives.
   - Appropriate funds for the U.S. Department of Commerce's Commercial Law Development Program (CLDP) to develop

model legislation and regulations for strategic investment and infrastructure reviews.

5. The Chinese government has steadily expanded its influence in the multilateral development banks (MDBs), raising its shareholding and voting power, increasing its contributions, and positioning itself to shape lending priorities and institutional governance. The United States has not used its position as a top shareholder, including its unique veto power over certain governance decisions at the World Bank, to effectively advance U.S. interests and hold these institutions accountable. In particular, the United States has a strong interest in ensuring that MDB funds do not disproportionately benefit Chinese firms, yet there is no comprehensive, regularly updated strategy or public accounting of procurement awards to Chinese and U.S. firms across all the MDBs.

   To focus engagement with international organizations—including international financial institutions (IFIs) and other multilateral institutions—on U.S. strategic interests and ensure adequate U.S. voice and representation at IFIs, Congress should:

   - Direct the Secretary of the Treasury, as Chair of the National Advisory Council on International Monetary and Financial Policies, to:
     - Submit to Congress a strategy within 180 days to leverage the U.S. voice and vote at the MDBs—the World Bank Group, the Inter-American Development Bank (IDB) and IDB Invest, the Asian Development Bank, the African Development Bank, and the European Bank for Reconstruction and Development—to counter China's action at IFIs and other multilateral institutions and to advance U.S. and democratic economic priorities, including responding to foreign adversaries' exploitation of IFIs. The strategy shall address, at a minimum:
       - The development of programs to expand participation by U.S. and allied suppliers, and U.S. technology alternatives to Chinese options, in MDB-financed projects and procurements, coordinated with existing commercial advocacy mechanisms, including the U.S. and Foreign Commercial Service and the Advocacy Center;
       - Supplier eligibility criteria grounded in security and technology provenance, together with an assessment of whether such criteria are required under each institution's existing procurement policy or would require action by its Board;
       - A plan to counter exploitation of these institutions by China and other foreign adversaries, addressed by category, including continued borrowing by countries eligible for graduation, concentration of procurement awards, bilateral co-financing vehicles, secondment and staffing, and incorporation of China's technical standards into project specifications; and

        - Measures to ensure transparency around beneficial ownership information for suppliers awarded financed contracts.
    - Meet at least once a quarter with the Secretaries of State and Commerce to discuss U.S. priorities for IFI engagement.
- Amend the annual report required by Section 1701 of the International Financial Institutions Act on International Monetary and Financial Policies (22 U.S.C. §262r) to require for each MDB disclosure of: (a) the value and number of contracts awarded to suppliers registered in the People's Republic of China (PRC) and to suppliers identified as controlled subsidiaries of PRC-domiciled parents, with Hong Kong and Macau reported separately; (b) contracts awarded under section (a) reported as a share of internationally completed procurement and disaggregated by sector and borrower country; and (c) a description of actions taken to heighten scrutiny of state-owned enterprise participation in MDB-financed procurement.
- Restrict travel funding for relevant offices to non-essential expenditures, for example, limiting premium-class travel, reception and event expenses, large delegations, conferences, and new discretionary initiatives, until the Administration nominates senior director positions.

6. Congress should authorize and appropriate dedicated funding, through the Secretary of State, Secretary of Homeland Security, or Secretary of Commerce, to expand the "Rip and Replace" initiative beyond domestic networks to key strategic partner nations and key regions of strategic competition, beginning with Latin America and the Indo-Pacific. The initiative should utilize novel methods and technology from across frontier labs to identify, expose, and harden against weaknesses in Chinese-origin technology and software. It should work with nations to modernize equipment either by replacing certain critical assets within network infrastructure or software to ensure trusted standards are established. Specifically, the initiative should include the following provisions:
    - Replace covered equipment. Building on the $8 million Panama pilot, fund the replacement of non-trusted telecommunications equipment in host nation infrastructure. Assistance should be conditioned on:
        - Host nation operational control of replacement systems and host government concurrence in public announcements;
        - A commitment not to reintroduce non-trusted equipment into assisted networks; and
        - Sustainment included in each project.
    - Assess, harden, and monitor software at scale. Direct the Secretaries of State and Homeland Security, drawing on the Defense Advanced Research Projects Agency (DARPA) and Na-

tional Security Agency (NSA), to apply artificial intelligence (AI)-enabled vulnerability discovery and patching to:

- Triage host nation exposure through analysis of Chinese-origin firmware and software, producing a prioritized queue;
- Identify and remediate vulnerabilities in the software on which replacement networks run, including AI-assisted rewriting of legacy code into memory-safe languages where source code is available; and
- Provide interim detection and monitoring of covered equipment awaiting replacement. Analysis of equipment originating in China should inform prioritization and monitoring.

Congress should authorize and appropriate the multiyear initiative to execute country-level projects and require annual reporting to the committees of jurisdiction on sites remediated, conditions enforced, partner cost-share, and any reintroduction of covered equipment.

7. Congress should make it U.S. policy that China's systematic use of Port State Control inspections and detentions of Panamanian-flagged vessels is economic coercion and authorize the President to take all necessary and appropriate economic actions to counter China and support the Government of Panama in this dispute, including leveraging existing sanctions authorities and initiating referrals to the International Maritime Organization to establish a record of China's weaponization of port access as a tool of geopolitical punishment.

   Congress should further direct the Federal Maritime Commission, which has already flagged the surge in detentions, to investigate the pattern and report findings within 90 days.

8. Congress should provide authorization and the necessary resources to the Secretaries of State, the Treasury, Defense, and Commerce to provide technical assistance to parliaments in Latin America to help draft and pass legislation to increase transparency and cybersecurity related to critical infrastructure through reforms to oversight, information security, and public contracting.

   To expose the cybersecurity risks, lack of investment, and other hazards in infrastructure facilities with Chinese technology and ownership, Congress should:

   - Direct the Director of National Intelligence to produce an annual unclassified assessment of, and brief other nations on, Chinese infrastructure presence across ports, energy, telecommunications, space, and other critical infrastructure sectors in the Western Hemisphere, including:
     - The security and economic risks associated with Chinese ports and equipment in the United States and countries in Latin America, including cybersecurity vulnerabilities, all potential vectors of military use and access, potential for economic lock-in effects and upcharges, and lack of capital investment.

- Direct the Secretary of State, in coordination with the Secretary of Defense, Secretary of Homeland Security, and U.S. Department of Transportation's Maritime Administration, to provide technical assistance to conduct inspections and establish a regional baseline for identifying and remediating vulnerabilities linked to China at strategic maritime chokepoints.
    - Where possible, the Secretary should seek cooperation with host countries for security audits of Chinese equipment and presence, identify highest-risk facilities, and recommend actions to ameliorate risk.

9. Across Latin America and the Caribbean, Chinese-linked criminal networks—money launderers servicing the region's cartels, illicit resource-extraction operations, and other currency channels that move value outside the correspondent banking system—have converged with an expanding PRC law enforcement presence that complicates, rather than supports, partner-nation cooperation with the United States.

   Congress should direct the President to establish and appoint an executive agent to identify, expose, and disrupt Chinese-linked illicit narcotics suppliers, money laundering organizations, cryptocurrency networks, resource extraction networks, and other criminal facilitators in Latin America and the Caribbean. The executive agent should address risks associated with Chinese police and law enforcement cooperation in the region and should focus on the following activities:

   - Disrupting Chinese money laundering networks.
   - Strengthening partner capacity.
   - Addressing risks from Chinese police training and security cooperation in the region.
   - Improving information sharing.

Chapter 5: Active Intercept: China's Efforts to Narrow U.S. Undersea Advantage

10. The Submarine Cable Act of 1888 only allows the United States to prosecute damage to subsea cables that occurs within U.S. territorial waters (i.e., within 12 nautical miles of its coastline) or damage caused by U.S.-flagged vessels wherever they operate. Current law limits the United States' ability to address other intentional damage to subsea cables landing in the United States or owned by U.S. entities. The United States must also address its limited repair ship capacity, which has led regulators to allow foreign adversaries to maintain U.S. cables that connect to the United States from a third country. This means provisions that would expand a trusted repair fleet and would ensure reinsurance for cable repair surge capacity during a crisis.

    To address adversarial attacks on critical U.S. telecommunications infrastructure in international waters, Congress should:

    - Amend the Submarine Cable Act to expand jurisdiction to prosecute acts of intentional sabotage against any critical un-

dersea infrastructure landing in the United States or having any ownership stakes from U.S. entities.

- Strengthen undersea cable repair capacity by:
  - Barring the use of foreign adversaries' repair ships on U.S. cables and directing regulators to take associated action;
  - In a manner consistent with current law, establishing a Pacific Allied Cable Repair Fleet, under which the Secretary of Transportation may enter operating agreements with qualified cable vessels flagged in the United States, and, where necessary, Japan, South Korea, and Taiwan; and
  - Directing the Secretary of Transportation to provide insurance or reinsurance against war risks for foreign vessels engaged in cable installation and repair, in coordination with allied countries when possible.

11. To combat the People's Republic of China's "Transparent Ocean" and undersea modernization efforts, Congress should:
    - Direct the Secretary of Defense, in consultation with the Director of National Intelligence and other relevant departments and agencies, to submit to the congressional defense committees a report, in both unclassified and classified versions, on China's "Transparent Ocean" efforts and associated programs. The reports should assess China's progress toward developing a persistent undersea surveillance architecture enabled by data fusion that integrates sensors and autonomous systems across domains from the seabed to space.

    To ensure the United States maintains its advantage over China in cutting-edge autonomous and semi-autonomous undersea systems, Congress should:
    - Direct the Secretary of Defense to submit to the congressional defense committees a classified report and briefing on its acquisition and program strategy for autonomous/semi-autonomous undersea systems. The report should address U.S. Department of Defense (DOD) capacity to surge production of these systems and detail how these platforms support U.S. Indo-Pacific Command's strategy in a Taiwan contingency.
    - Appropriate funds for DOD to conduct a competitive, multi-supplier uncrewed underwater vehicle (UUV) hull-manufacturing qualification pilot that expands the industrial base beyond established defense contractors.
    - Appropriate funds to expand DOD and other U.S. government agencies' procurement of UUVs. These agencies could include those falling under the U.S. Department of Commerce, U.S. Department of Homeland Security, U.S. Department of the Interior, and U.S. Environmental Protection Agency.
12. To maintain U.S. advantage in undersea surveying and seabed mapping, Congress should authorize and appropriate additional funds to the U.S. Department of Commerce's National Oceanic and Atmospheric Administration (NOAA) to expand seabed surveys and mapping operations in the Pacific, with a focus on

working with the governments of the Pacific Island countries to conduct surveys in their exclusive economic zones (EEZs).

- An agreement with a country under this initiative should condition cooperation on prohibiting Chinese research vessel exploratory activity, seabed mapping, and seabed mining in its waters to the maximum extent permitted.

Chapter 6: The Price of Everything: China's Bid to Reshape Global Commodities Markets

13. For over two decades, China has quietly pursued the development of domestic commodities exchanges, and expanded its production and processing of core commodities, becoming a key market maker in many segments and sectors. China is actively working to exert greater influence over global commodities markets with the aim of advantaging its domestic manufacturers and insulating itself against U.S. sanctions. To this end, China is pursuing numerous policies to expand its leverage, growing its domestic commodity exchanges, and opening more "in China for China" commodities trading to foreign participants. In recent years, China established the China Mineral Resources Group and other state instruments to consolidate purchasing of key commodities and has begun leveraging its position as a major buyer in physical markets to compel producers to use its preferred benchmarks and, in some cases, transact in RMB. China is building parallel systems that, absent action, may, over time, reshape the global landscape.

    Congress should direct the U.S. Commodity Futures Trading Commission (CFTC) to monitor Chinese engagement and influence in commodities exchanges and warehousing and provide an annual report to Congress on activity, strategic risks, and efforts to coerce market participants as well as signs of market manipulation. To support this activity, Congress should:

    - Expand CFTC foreign market surveillance and provide the CFTC the direction and, as needed, authority to monitor trading activity on Chinese exchanges, including but not limited to the Dalian Commodity Exchange (DCE) and the Shanghai International Energy Exchange (INE), with particular attention to participant concentration, state-owned enterprise positioning, and coordination among state-owned buyers. Current CFTC jurisdictional limits leave this activity unmonitored, and the China Securities Regulatory Commission does not make these data public.
    - Direct the CFTC to monitor the development of China's futures markets, in particular for semiconductor, battery, renewable energy, and critical industrial materials. Data on commodity pricing are difficult to obtain, particularly in markets where benchmark usage and settlement terms are embedded in opaque, privately negotiated contracts and are not systematically reported. Thinly traded contracts are susceptible to a risk of biased market data, putting U.S. producers at a disadvantage.

- Require disclosure of U.S. financial institution exposure to Chinese exchanges and other non-CFTC-registered foreign exchanges, as appropriate. Dodd-Frank reporting captures most U.S. derivatives activity on domestic and CFTC-registered foreign exchanges; however, many Chinese exchanges, including the INE, fall outside this framework, and these exchanges have not sought CFTC registration as Foreign Boards of Trade, meaning U.S. firms can trade on them without that activity being systematically captured in CFTC reporting.

14. Congress should strengthen the U.S. Department of Agriculture's (USDA) agricultural market intelligence and early warning capacity by directing the Secretary of Agriculture to enhance USDA's capacity to monitor Chinese agricultural commodity markets, supply chain flows, and state reserve management—such as dedicated monitoring of the Dalian Commodity Exchange's price signals and South American logistical flows controlled by Chinese-affiliated entities—and by providing sufficient appropriations to do so.

Part III: China's Technology Ambitions

Chapter 7: Collect, Steal, Buy, Fuse, Monetize: How China Is Turning Data into Assets and Ammunition

15. Data are a strategic asset that can drive scientific discovery, economic growth, and national security, but their value depends on the ability to organize, protect, and use them effectively. The United States needs a coordinated framework that makes data more accessible for legitimate uses, gives Americans control over their personal data, and prevents exploitation by China and other adversaries. An American Data Initiative would advance these goals while providing Americans meaningful control over their personal data.

    Congress should establish an American Data Initiative to put American data to work as a source of national power, while preserving decentralized ownership, giving Americans control over their own data, and keeping their data out of the hands of China and other adversaries. Congress should:

    Organize Federal Data

    - Make the Administrator of General Services the Federal Chief Data Officer, with binding standards authority over all agencies and every agency Chief Data Officer appointed by and reporting to the Administrator, after consultation with the agency head.
    - Direct the Administrator to govern all federal data by sensitivity and value, including in aggregate, and to make Data.gov the catalog of all federal data, open by default, with registered access for non-public data.
    - Direct the Administrator to establish sectoral data foundries that produce AI-ready datasets, beginning with biology and embodied AI.

- Require the Administrator's approval of agency data budgets and bar funding for noncompliant data systems.
- Apply the confidentiality protections of Title 13 to personal data shared through the Initiative and record every access to non-public federal data in a tamper-proof log.
- Give the Government Accountability Office continuous access to those logs and authority to review any access to personal data and require an annual report to Congress with agency scorecards and privacy and civil liberties compliance audited by the Government Accountability Office.

Put Data on the Balance Sheet

- Make it U.S. policy that data held by federal agencies and U.S. businesses are an asset recognized on the balance sheet.
- Direct the U.S. Securities and Exchange Commission to require the Financial Accounting Standards Board to set standards for recognizing data as an asset within two years.
- Direct the Federal Accounting Standards Advisory Board to set comparable standards for federal agencies.
- Direct the Public Company Accounting Oversight Board to set matching audit standards.
- Direct the federal banking regulators to exclude data assets from regulatory capital.
- Condition the Governmental Accounting Standards Board's federal funding on comparable standards for state and local governments.

Let Americans Decide Who Gets Their Data

- Codify the core prohibitions of the U.S. Department of Justice's Data Security Program, including its bars on giving China and other countries of concern and covered persons access to Americans' bulk sensitive personal data and government-related data and its limits on onward transfer, and leave compliance requirements to regulation.
- Direct the President to designate an appropriate Cabinet or agency official to establish a national opt-in program under which data brokers may not sell, license, or share Americans' personal data unless the consumer has opted in through a single federal portal that brokers must check before any transfer.
- Extend the Protecting Americans' Data from Foreign Adversaries Act to require data brokers, under a common statutory definition that applies throughout the Initiative and includes resellers and other intermediaries, to register with the designated official, hold them liable for transfers made without consent, bar transfers to persons under the jurisdiction of China or another foreign adversary regardless of consent, and make these obligations follow the data through every resale.
- Require data brokers, within two years, to obtain consent for personal data they already hold or delete it.

Bring Data Sales Out of the Shadows

- Define the rights in data that companies, governments, and consenting individuals can buy, sell, and license.
- Direct the designated official to register and supervise data exchanges, require data brokers, within two years, to sell personal data only through registered exchanges, and require exchanges to verify data provenance and consumer consent, screen buyers for ties to China and other foreign adversaries, including beneficial ownership and intended use, keep auditable records of every transfer, bar unauthorized resale and improper data combination, bar onward transfers to third countries without equivalent controls, meet security standards, and bar participants under foreign-adversary jurisdiction.
- Direct the Secretary of Commerce to open U.S. data exchanges to participants from allied and partner countries whose governments adopt equivalent consent, provenance, and foreign-adversary screening rules and extend reciprocal access to U.S. participants.

16. In 2024, the Commission recommended that Congress codify the authority established under the "Securing the Information and Communications Technology and Services Supply Chain" Executive Order (ICTS). The Connected Vehicle Rule demonstrates that the ICTS framework can work but it lacks a statutory basis and congressional direction to regularly identify, assess and mitigate risks across high-risk technology sectors.

    Congress should codify the U.S. Department of Commerce's Office of Information and Communications Technology and Services (OICTS) and its ICTS authorities, provide dedicated funding and personnel, and require the office, in coordination with relevant federal agencies, to:

    - Regularly assess categories of foreign-adversary information and communications technologies and services that could expose sensitive U.S. data, enable remote access or control, or compromise U.S. critical infrastructure.
    - Report findings and proposed mitigation measures to Congress and initiate rulemaking for sectors posing national security risks, or explain why regulatory action is unwarranted.

17. To prevent China from stealing American data and harming American companies, Congress should establish a systematic effort against the ecosystem that supplies and monetizes China's cyber intrusions using "hackers for hire" and commercial cyber actors, by taking the following actions:

    - Direct the National Cyber Director, in coordination with the Director of the Cybersecurity and Infrastructure Agency, the Director of the Federal Bureau of Investigation, the Director of National Intelligence, and the Secretaries of State, Treasury, Commerce, and Defense, to publish annually a list of foreign persons that:

- Knowingly supply data, intrusion software, and botnet services to China's state-sponsored cyber actors or "hackers for hire";
- Acquire or commercialize data or intellectual property stolen through those operations; or
- Act as subsidiaries, affiliates, partners, joint ventures, licensees, or significant subcontractors of covered entities.

- Require within the 180-day period after the publication of each annual list:
  - The Secretaries of Treasury and State to determine whether blocking, financial, or visa sanctions are warranted;
  - The Secretary of Defense to determine whether government-wide or defense-specific procurement exclusion is warranted; and
  - The Chair of the Federal Communications Commission, where communications equipment or services are involved, to determine whether Covered List inclusion is warranted based on a determination by an authorized federal entity.
- Establish a program that would allow designated U.S. private sector entities to conduct cyber operations against approved foreign entities.
- Require reporting to the relevant committees of Congress, on: whether sanctions were imposed or list placements made; any identified statutory or resource gaps; enforcement coordination with allies; beneficial ownership and affiliate information; and procurement exposure across federal agencies.

Chapter 8: Silicon to Sovereignty: China's Bid to Control the AI Stack from Wafer to Weights, Part One

18. The growing proliferation and adoption of Chinese open-weight artificial intelligence (AI) models in the United States carries national security implications for sensitive data, cybersecurity, and dependence on Chinese technology. Uncertainty about how these models behave in sensitive applications, what vulnerabilities they may introduce, and whether safeguards can adequately mitigate those risks warrants greater federal scrutiny. Congress should require enforceable protections for sensitive applications before these models become embedded in critical systems and costly to replace.

    Congress should require the Secretary of Commerce, through the Office of Information and Communications Technology and Services (OICTS), in coordination with the Center for Advancing Innovation and Standards for Super Intelligence (CAISSI) and relevant federal agencies, to:

    - Restrict deployment in sensitive applications unless safeguards are demonstrated. Within 180 days, identify sensitive uses—including systems controlling critical infrastructure, performing national security functions, or processing bulk sensitive personal data—and prohibit new deployment of cov-

ered models in those uses absent a time-limited authorization based on independently evaluated safeguards. Authorizations should address the model, its deployment environment, and its access to data, networks, and tools.

- Require identification and mitigation of existing exposure. Direct federal agencies and covered operators in designated sensitive sectors to inventory existing deployments and implement enforceable mitigation or replacement plans within deadlines established by the Secretary.
- Establish continuing security obligations. Require independent security testing, reporting of significant security incidents, reassessment following material modifications, and verification of compliance. Direct the Secretary to restrict or prohibit the commercial provision or deployment of designated models where identified risks cannot be adequately mitigated.
- Reduce strategic dependence. Require providers serving designated sensitive applications to maintain documented capabilities to replace covered models and migrate affected systems and data to alternatives meeting federal security requirements.

Within 180 days, the Secretary should also complete a consolidated assessment, building on existing federal evaluations, the National Telecommunications and Information Administration's (NTIA) open-model assessment, and federal supply-chain restrictions. The assessment should distinguish risks inherent in model weights from those arising from hosting, software, updates, and system integration; identify gaps in testing and verification; and inform subsequent requirements without delaying initial implementation.

Congress should authorize and appropriate funding, information-gathering and enforcement authorities, and penalties for noncompliance. The legislation should provide narrowly tailored exceptions for security research and authorized national security activities and require annual reporting to Congress on deployment exposure, compliance, mitigation effectiveness, and remaining dependencies.

19. Americans should know when the government services they receive and the commercial products they use rely on AI models developed by Chinese companies. Clear disclosure would help consumers, businesses, and investors assess potential risks to data security, privacy, service reliability, and national security.

Congress should make it U.S. policy that Americans know when governments and businesses rely on AI models developed by Chinese companies. Congress should:

- Require federal agencies, and any state or local government or other entity that receives federal funds or federal tax credits, to disclose any use of AI models developed by an entity headquartered in, or organized under the laws of China, or owned or controlled by such an entity, including models fine-tuned

on or derived from them, wherever they are hosted. Disclosure should appear in clear language on their public-facing platforms and in their filings with the federal government.

- Require businesses that use such models in any part of a product or service offered in the United States to consumers or other businesses to disclose that use clearly on their websites and in product documentation and treat failure to disclose as an unfair or deceptive act or practice enforceable by the Federal Trade Commission.
- Require reporting companies, as part of quarterly and annual disclosure filings with the U.S. Securities and Exchange Commission, to disclose as a material business risk the extent of their use of such models.

20. Sustaining U.S. leadership in AI requires reliable access to advanced chips and the manufacturing capacity needed to produce them. Exports to China should not come at the expense of capacity needed to support U.S. AI development and deployment. Requiring auditable exporter certifications would help ensure that export decisions account for these constraints and protect U.S. access to critical capacity.

    Congress should ensure that AI chip exports to China do not divert capacity from the U.S. market, including by amending the Export Control Reform Act of 2018 (ECRA) to condition exports, reexports, or in-country transfers of advanced AI chips to China on exporter certification that they will not divert advanced semiconductor manufacturing or AI capacity from the U.S. market. The legislation should:

    - Cover upstream capacity, including advanced-node wafer fabrication, high-bandwidth memory, and advanced packaging—not finished-chip inventory alone;
    - Require auditable capacity-allocation data submitted to the Bureau of Industry and Security, subject to ECRA record-keeping and enforcement provisions, including criminal penalties for false certification;
    - Require the Bureau of Industry and Security to report annually to the committees of jurisdiction on certifications, validation methods, and exports coinciding with unmet U.S. or allied demand for equivalent capacity; and
    - Prohibit regulatory waivers or narrowing of the requirement without an affirmative national security determination transmitted to Congress for a 30-day review period.

Part IV: Taiwan and Hong Kong

Chapter 9: Taiwan: A Crucial Window for a Critical Partner

21. The People's Republic of China's (PRC) aggressive actions to reshape the Western Pacific and force unification with Taiwan are intensifying. Yet much U.S. and allied contingency planning focuses on large-scale invasion scenarios rather than coercion below the threshold of war. The United States needs a coordinated

playbook with allies and partners for responding to a range of coercive gray zone activities by the PRC in the Indo-Pacific, specifically concerning Taiwan.

Congress should:

- Direct the National Security Advisor to develop a common playbook with allies and partners calibrated to counter multi-domain day-to-day PRC coercion. Departments and agencies involved in executing the playbook should develop tiger teams to address U.S. actions and coalition/allied actions under each area of responsibility. That playbook should provide a unified framework for participating nations to:
  - Share situational awareness and arrange pre-coordinated responses;
  - Counter disinformation and lawfare;
  - Expand combined coast guard operations with Taiwan and regional partners, including through multilateral initiatives; and
  - Support resistance against economic coercion.
- Amend and extend the Taiwan Enhanced Resilience Act to establish a Taiwan Democratic Resilience Initiative led by the U.S. Department of State, implemented through the American Institute in Taiwan in coordination with the Office of the Director of National Intelligence and other appropriate departments and agencies.
  - The Initiative should strengthen U.S.-Taiwan cooperation to support the resiliency of Taiwan's civil society and counter PRC united front activities, election interference, and disinformation campaigns. It should also include information sharing with U.S. allies and partners.
- Direct the National Security Advisor to lead an interagency process to develop a whole of government strategy for deterring, preparing for, and responding to coercive actions by the PRC against Taiwan that are intended to rapidly or substantially alter the status quo, but that fall below the threshold of a large-scale invasion or armed conflict.
  - It should include an assessment of contingency scenarios and for each, provide an assessment of indicators and warnings, likely PRC objectives, decision points, escalation risks, potential effects on Taiwan's access to critical goods and services, and options for coordinated actions with allies and partners.

22. As China's military capabilities expand and the regional balance of power shifts, the risk of conflict in the Western Pacific is increasing. Despite growing defense cooperation among the United States and its allies and partners, the absence of a formal multilateral security framework limits their ability to deter aggression and mount a coordinated response to attempts to alter the regional order by force.

Congress should direct the Secretaries of Defense and State to initiate consultations with U.S. allies on establishing a formal multilateral framework for collective defense in the Western Pacific, building on the multilateral defense cooperation directed by Section 1254 of the fiscal year 2026 National Defense Authorization Act. Where Section 1254 directs operational integration, this framework would institutionalize the political commitment to collective action needed to deter Chinese military aggression and provide the foundation for a Western Pacific Security Pact. The Pact should:

- Build on existing regional defense mechanisms among states with established foundations for expanded multilateral defense cooperation, primarily the U.S.-Japan-Australia-Philippines Defense Cooperation Council, and be positioned to complement multilateral security frameworks such as the Quad and AUKUS. Provide a pathway for accession by other states that share the Pact's principles and possess the willingness and capacity to contribute materially to peace, security, and collective defense in the Western Pacific.
- Establish a common commitment to collective defense under which members recognize that any major threat to, or violent breach of, peace and stability in the Western Pacific—or any military attack upon the members of this framework—threatens their shared security and national interests and commit to coordinate a powerful collective response to deter or defeat aggression and restore regional peace and stability.
- Accelerate the legal and military reforms necessary for collective defense, including combined contingency planning and exercises, integrated command and control, expanded intelligence sharing, reciprocal access, and integrated logistics to enable members to operate effectively as a combined force in crisis or conflict.

23. Beijing is using travel bans and other punitive measures to deter and intimidate foreign lawmakers from engaging with Taiwan, including barring four New Zealand legislators from the People's Republic of China in June 2026. By placing exchanges with Taiwan on the same footing as those with the UK, Canada, and Mexico, Congress would signal that parliamentary diplomacy with fellow democracies is routine, legitimate, and not subject to Beijing's veto.

    The U.S. House of Representatives and Senate, respectively, should establish U.S.-Taiwan Inter-Parliamentary Exchanges, modeled on the established bilateral exchanges with the UK, Canada, and Mexico.

    - Like those bodies, the exchanges would convene regular, structured meetings between members of the U.S. legislative branch and members of Taiwan's Legislative Yuan to discuss trade, security, technology, and shared democratic governance.

24. Taiwan is rapidly scaling its civilian and defense drone industries, building asymmetric capability that will be critical to prevailing in a potential future conflict with the People's Republic

of China. Recent U.S. actions to broadly prohibit foreign drone imports stand to restrict a key market for Taiwan's drone makers and limit mutually beneficial collaboration with U.S. manufacturers.

Recognizing the benefit to U.S. national security of supporting drone industries of allies and partners at risk of conflict with adversarial countries, Congress should direct the Federal Communications Commission to limit its December 22, 2025 addition to the Covered List of uncrewed aircraft systems and their critical components, to systems and components produced by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, as defined in 15 CFR § 791.4.

Chapter 10: Hong Kong: Enabler of China's Global Finance and Technology Ambitions

25. Hong Kong's legal environment is deteriorating—not in a single dramatic event but through continuous, layered legislation that changes business risk year after year. Virtually any legal dispute involving a U.S. firm or its staff could be channeled into a national security case, and only a recurring statutory assessment keeps U.S. businesses informed.

    Congress should require the Secretaries of State, the Treasury, and Commerce to jointly issue an annual Hong Kong Business Advisory informing U.S. firms of the legal, regulatory, financial, and reputational risks of operating in the Hong Kong Special Administrative Region. Each advisory would include the following:

    - An assessment of developments over the preceding year, including new legislation, subsidiary regulations, enforcement actions, erosion of the rule of law, sanctions and/or export control evasion activities, and exit restriction risks.
    - Updated guidance on risk exposure for personnel, data, intellectual property, and operations.

26. The U.S. Department of the Treasury has identified Hong Kong-based entities as key enablers of crypto-facilitated Iranian oil revenue laundering.

    Congress should enact legislation to apply Primary Money Laundering Concern special measures, including correspondent account prohibitions, on Hong Kong Virtual Asset Service Providers that fail to prevent Iranian, Russian, or North Korean cryptocurrency trades.

Other Recommendations

The following recommendations build upon the Commission's work in recent years, including research, briefings, fact-finding trips, and conversations with key stakeholders.

27. The Commission reaffirms its 2025 recommendation on post-quantum cryptography. Post-quantum risk is coming faster than the government is acting, and the federal response does not yet match the threat. China is investing heavily in quantum

computing and has demonstrated sustained, large-scale collection against U.S. government networks. What Beijing steals encrypted today, it can read once a cryptographically relevant quantum computer exists. That same capability would also allow adversaries to forge the digital signatures that authenticate federal software, firmware, and certificates. The U.S. Government Accountability Office reports that agencies are only beginning migration, citing gaps in expertise, inventories, funding, and testing plans. At this pace, the government will miss its own 2030 target for critical systems. The government needs to treat this with far greater urgency.

Congress should:

- Require by statute that federal agencies migrate high-value assets, Federal Information Security Modernization Act (FISMA) high-impact systems, and public key infrastructure—including root certificate authorities and code- and firmware-signing systems—to National Institute of Standards and Technology (NIST)-approved post-quantum cryptography within 24 months of enactment. The statute should also set an accelerated, binding schedule for all remaining unclassified systems.
- Establish a dedicated post-quantum migration appropriation, separate from agency cybersecurity budgets, based on agency cost estimates certified by the Office of Management and Budget.
- Fund NIST's Cryptographic Module Validation Program and Cryptographic Algorithm Validation Program at levels sufficient to reduce validation wait times for post-quantum products.
- Require agency heads to certify progress to Congress every six months, with signed waivers for any missed milestone.
- Make crypto-agility and vendor post-quantum roadmaps conditions of federal information technology procurement.

28. People's Republic of China censorship demands on American companies are delivered privately and complied with quietly, leaving Congress, regulators, investors, and the public with no systematic picture of how widely Beijing's speech controls are being exported into the operations of U.S. firms. Mandatory disclosure corrects this information failure at minimal cost: it prohibits no transaction and forces no confrontation with Chinese law, yet it strips censorship demands of the secrecy they depend on, gives every firm legal cover to report rather than forcing each to choose transparency on their own, and equips U.S. policymakers with comprehensive data for trade and human-rights diplomacy.

Congress should:

- Require all U.S. firms operating in or doing business with the People's Republic of China to disclose to the Secretary of State and Secretary of Commerce and to each of the four congressional leaders every order, request, or directive re-

ceived from Chinese government officials or their agents to censor, block, remove, or otherwise suppress free expression, including content directed at users outside China, within one month of each such request.

- Direct the Chair of the U.S. Securities and Exchange Commission to require reporting companies to disclose in annual and quarterly filings every order, request, or directive received from Chinese government officials or their agents to censor, block, remove, or otherwise suppress free expression, including content directed at users outside China.

29. As China expands its activities in space, the United States must be able to move at the speed of relevance to share intelligence with allies and partners in instances where such releases would strengthen collective action vis-à-vis China on space matters, while safeguarding sensitive sources and methods.

    Congress should direct the Director of National Intelligence to work with the Secretary of State and other relevant executive branch agencies to create a process for accelerating the releasability of intelligence related to Chinese space activities to allied and partner nations that can favorably support U.S. competitive posture on space matters.

30. To expand defense technology cooperation and interoperability with trusted countries, Congress should:

    - Make it U.S. policy to establish a standing partner track under AUKUS Pillar II.
    - Direct the Secretary of State to propose the partner track to Australia and the UK.
    - Condition partner track access on security benchmarks the Secretary of State certifies to Congress annually, including protection against access by persons under foreign adversary jurisdiction.