



FOREIGN AFFAIRS
COMMITTEE

CHAIRMAN MCCAUL

Bureau of Industry & Security: 90-Day Review Report

Chairman Michael McCaul



TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	1
INCREASING BIPARTISAN CONSENSUS.....	2
CRITICAL ROLE OF EMERGING TECHNOLOGIES.....	3
REEMERGENCE OF EXPORT CONTROLS IN STRATEGIC COMPETITION.....	5
BACKGROUND ON EXPORT CONTROLS.....	7
ENHANCED EQUITY ON THE OPERATING COMMITTEE.....	14
MODERNIZED LICENSING POLICY FOR CHINA.....	18
UPDATED ENTITY LIST REQUIREMENTS.....	23
REINVIGORATED PLURILATERAL CONTROLS.....	30
STRENGTHENED END-USE CHECKS, ENFORCEMENT, AND OVERSIGHT.....	32
CONCLUSION.....	46
APPENDICES.....	47
APPENDIX I — RECOMMENDATIONS.....	47
APPENDIX II — ORGANIZATIONAL CHART.....	51
APPENDIX III — DEFINITIONS.....	52



EXECUTIVE SUMMARY

We can no longer afford to avoid the truth: the unimpeded transfer of U.S. technology to China is one of the single-largest contributors to China's emergence as one of the world's premier scientific and technological powers. For more than 20 years, the Chinese Communist Party (CCP) has circumvented our export controls and deceived the U.S. officials in charge of administering them. While U.S. officials were pursuing economic engagement, China was executing a path toward technological independence.

In 2006, China launched its "indigenous innovation" strategy aimed at making China a science, technology, and innovation superpower. Since then, state planners issued numerous industrial policies, such as "the Medium- and Long-Term Scientific Plan," "Strategic Emerging Industries," "Made in China 2025," and "Dual-Circulation." Each plan had its own focus, but the mission was always the same: supplant U.S. technological leadership. The United States now stands at an impasse: having let U.S. export control officials fuel the technological and manufacturing rise of China in the pursuit of short-term industry profit, do we make the necessary modernizations at the Department of Commerce's Bureau of Industry and Security, or do we hope for the best with the status quo?



INCREASING BIPARTISAN CONSENSUS

Multiple U.S. administrations have come to the same conclusion that China aims to change how the world operates—from how we trade to how democratic societies express their values. To achieve this goal, the CCP General Secretary, Xi Jinping, has not ruled out the use of his military and has directed his government to use China’s economic and technological base as a blunt, coercive tool.

The CCP is in the boardroom and laboratory of nearly every organization in China, even notionally private ones and American companies,ⁱ to influence decision making. The world must accept that the economic and innovation engine in China is driving toward the Great Rejuvenation of the Chinese Nation—a CCP plan to have a military second to none and to bring democratic Taiwan under its control. These actions are forcing countries to reexamine the view that trade and commerce can be distinct and separate from national security.

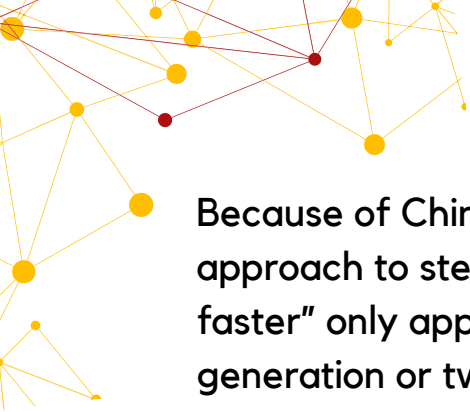
In 2017, the U.S. National Security Strategy reasserted that “economic security is national security,”ⁱⁱ a view that guided our country during its founding.ⁱⁱⁱ It is evident that economic and manufacturing strength is the foundation for our military and diplomacy. Today’s breakneck pace of innovation in certain emerging technologies creates an opportunity for adversaries like the CCP to disrupt the balance of economic and military power.



CRITICAL ROLE OF EMERGING TECHNOLOGIES

The stakes could not be higher. Indeed, the U.S. intelligence community assesses that critical and emerging technologies such as quantum, artificial intelligence (AI), and biotechnology may determine superpower status in the 21st century.^{iv} As these technologies are dual-use—meaning they have both benign, productive uses as well as malign, destructive ones—the United States and other rules-based countries must lead their research, development, and production. Concerningly, China is reportedly leading in 37 out of 44 critical technologies,^v and it is implementing an unprecedented, zero-sum industrial policy to gain dominant market share by investing hundreds of billions of dollars and building a more aggressive technology transfer regime.

The United States must have a win-at-all-costs mentality in these emerging technologies. In the Cold War, the United States made landing on the moon first and denying and delaying the Soviet Union's access to technology a national mission. Prior to serving in the Biden administration, several current national security officials, including some at the National Security Council, wrote that managing the China Challenge “should be an organizing principle of U.S. foreign policy”—resembling a competitive mindset the United States had toward the Soviet Union.^{vi}



Because of China’s massive industrial subsidies and comprehensive approach to stealing and inducing the transfer of technology, a “run faster” only approach—which relies on innovating faster and staying a generation or two ahead of competitors—will fail on its own against China.^{vii}

Instead, the United States must invest in innovation while denying and delaying China’s access to critical technologies. Consequently, export controls are reemerging as a vital tool in the U.S. national security and foreign policy toolkit.

Despite China’s strengths, it has several technology chokepoints—areas in which it is reliant on the United States or other countries for foundational technology. Semiconductors are an illustrative example. Up and down the supply and value chain, China cannot independently produce advanced semiconductors without the talent, know-how, and technology of a small group of democratic countries. If the United States and a handful of U.S. treaty allies fully restricted China’s access to semiconductor architecture, electronic design automation software, machine tools, and fabrication facilities—foundational technologies—then China’s silicon ambitions may become prohibitively costly and time-intensive.



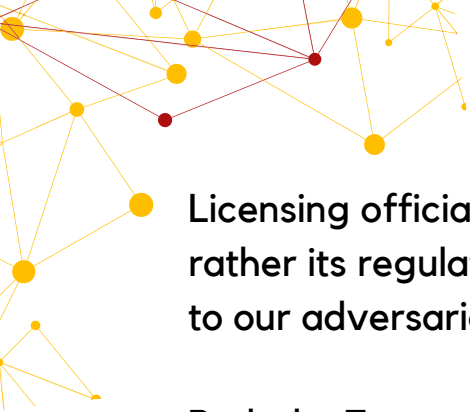
REEMERGENCE OF EXPORT CONTROLS IN STRATEGIC COMPETITION

The United States has a narrowing window in which export controls can redirect the development of ecosystems and production of emerging technologies away from China. To accomplish this, we can no longer accept an export control bureaucracy that is reactive to technological advances and fails to impose controls on emerging technology until that technology is being weaponized. Export controls must be used more as a preemptive tool to safeguard against technology transfers that may appear benign today, but have the potential to threaten national and economic security in the future.

Consequently, the United States can no longer outsource its economic statecraft to a global free market, dictated largely by China's industrial policies. Instead, the U.S. government must take a more active role in fencing off the CCP's commercial activity that threatens our security. At the same time, the United States and its allies and partners must act together to be the preeminent technological superpowers to constrain China from achieving the same goal.

This report will provide an overview of the U.S. export control regime housed at the Department of Commerce, explain China's distinct and growing threat, and offer policy recommendations.

In short, if the United States is determined to outcompete China, the fossilized licensing bureaucracy that oversees export controls must break free from its post-Cold War, free trade mentality. It must regain its *raison d'être* in identifying and controlling technology and being the vanguard of strategic competition.



Licensing officials cannot see themselves as the voice of business, but rather its regulator more willing to deny licenses to export technology to our adversaries.

Both the Trump and Biden administrations, principally from the White House, have rightly begun exerting more control over the Commerce Department's Bureau of Industry and Security (BIS). However, no administration will be able to fully leverage the power of export controls to protect U.S. national security without Congressional action. Now, Congress must solidify the efforts of successive administrations so our future will be better secured.



BACKGROUND ON EXPORT CONTROLS

U.S. Views on Technology Competition with China

In multiple documents and statements, the U.S. government has asserted that technology is central to U.S.-China strategic competition. The U.S. National Counterintelligence and Security Center wrote that leadership in a few technology sectors, including AI, semiconductors, and quantum, may determine whether America remains a superpower or is eclipsed by strategic competitors—no doubt an allusion to China.^{viii} CIA Director Bill Burns told Congress, “I think the revolution in technology is...the main area for competition with the People’s Republic of China.”^{ix} The Department of Defense warns that “China is particularly focused on dominating a range of emerging, dual-use technologies that promise to be both disruptive and foundational for future economies.”^x

Core to U.S. policy with respect to the People’s Republic of China (PRC), consistent over successive administrations, are the concepts that “economic security is national security”^{xi} and that export controls are a “new strategic asset” to use against adversaries.^{xii} These policies did not emerge randomly; instead, CCP behaviors and actions reinvigorated these concepts and tools that had been hibernating since the fall of the Soviet Union.

CCP Views on Technology Competition

The General Secretary of the CCP Xi Jinping believes technology and innovation are critical to his concept of comprehensive national security, saying “advanced technology is the sharp weapon of the modern state.”^{xiii}




General Secretary Xi's Great Rejuvenation of the Chinese Nation requires "core technologies must be held in our own hands."^{xiv}

General Secretary Xi's conviction that technology may help China leapfrog the United States in power and influence makes him more willing to accept costs and use coercion to achieve his goals.^{xv} The U.S. Chamber of Commerce has written that China is "leverag[ing] the power of the state to alter dynamics in global markets in industries core to economic competitiveness."^{xvi} The Mercator Institute, a German think tank, warned that China is trying "to systematically acquire cutting-edge technology and generate large-scale technology transfer."^{xvii}

Power over the Chinese economy and its technological goals, therefore, is central to Xi's national security vision. For more than 10 years, General Secretary Xi has built a formidable, interlocking legal and regulatory system that makes access to his market dependent on transferring private sector technology, data, and know-how to the Chinese government—and eventually their Chinese competitors.

Military-Civil Fusion and Export Controls

The clear, direct link between China's economy and its military make the technology transfer system a threat to U.S. national and economic security. The CCP, its People's Liberation Army (PLA), and the government are using trade and commerce to seize dominant market share and manufacturing capability in dual-use technologies that will define the future of warfare and the global economy.^{xviii} The CCP's Military-Civil Fusion Strategy (MCF) ensures that any militarily useful technology developed or acquired by the private sector can be diverted to the PLA.^{xix}



Former Acting Under Secretary at the Department of State Dr. Christopher Ashley Ford summarized MCF perfectly:

"If any given technology is in any way accessible to China...and officials there believe it can be of any use to the country's military and national security complex as Beijing prepares itself to challenge the United States for global leadership, one can be quite sure that the technology will be made available for those purposes – pretty much no matter what."^{xx}

General Secretary Xi is in effect marshaling the world's second largest economy and second largest recipient of foreign direct investment to create a more lethal military. A military that Xi says may be used to take back control of Taiwan or control shipping lanes that carry more than \$5 trillion worth of goods.^{xxi}

The Congressional Research Service explained that "China's approach [i.e. MCF] blurs commercial and military distinctions and may challenge the U.S. export control regime's ability to distinguish between military and civilian end-use and end-users."^{xxii} Former Acting Under Secretary of BIS Nazak Nikakhtar related MCF to export controls saying, "(e)xpport control regimes are based entirely on trust—trust that the end-user recipient of the item will not re-export the item to prohibited end-users or for prohibited end-uses."^{xxiii} MCF subverts the trust that is the foundation of the global trading system.

MCF combined with China's existing laws and regulations—including its blocking regulations and 2017 National Intelligence Law—create contradictory legal requirements for companies doing business in China and the United States. For example, a recipient of U.S.-origin technology in China may be required by China's law to divert that technology to the government or military and at the same time be required by U.S. law not to divert such technology to any other end-user.



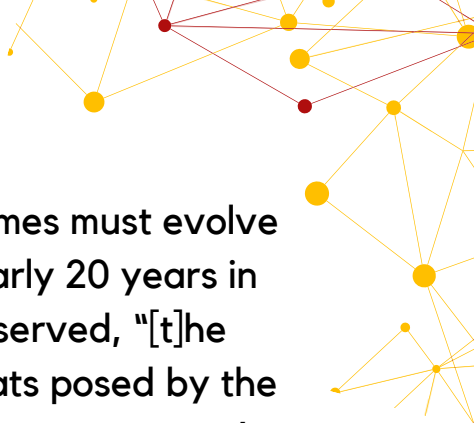
Companies cannot comply with both sets of laws. Furthermore, finding and enforcing violations of U.S. laws in China may not be possible because of the closed, opaque system in China.

China's Violation of Commitments

China's track record of abiding by commitments made bilaterally with the United States or multilaterally through international organizations, such as the World Trade Organization, raises significant doubt that the U.S. government could trust any export control end-use agreements in China. China violated commitments not to militarize the South China Sea, to respect treaty obligations regarding Hong Kong, and has denied its ongoing genocide in Xinjiang. Moreover, China steals annually upwards of \$600 billion worth of American intellectual property.^{xxiv} In 2023 the Office of the U.S. Trade Representative in its annual Special 301 report articulated that regulatory regimes are being used to require inappropriate disclosure of trade secrets and other types of intellectual property.^{xxv}

Given China's track record of violating bilateral commitments, Steve Coonen, a former senior foreign affairs advisor for the Defense Technology Security Administration at the Department of Defense, asks, "Why do U.S. export control officials imagine that these same leaders will honor end-user conditions for technologies that the PLA and MSS [Ministry of State Security] need?"^{xxvi}

For these reasons, U.S. export control officials should adopt a presumption that all PRC entities will divert technology to military or surveillance uses. Currently, the overwhelming approval rates for licenses or exceptions for dual-use technology transfers to China indicate that licensing officials at BIS are likely presuming that items will be used only for their intended purposes.

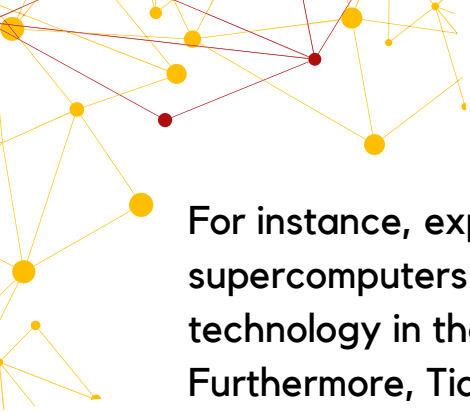


Some experts believe the U.S. legal and regulatory regimes must evolve to protect U.S. technology. Jeffrey Stoff, who spent nearly 20 years in the U.S. government as a China analyst and linguist, observed, “[t]he scale and scope of national and economic security threats posed by the PRC’s technology transfer apparatus have outpaced the government’s abilities or priorities to detect, deter, or neutralize the PRC’s efforts.”^{xxvii} A core finding of his research is that many threats from the PRC are “neither criminal in nature nor involve espionage, at least not how our legal system defines it.”^{xxviii} If the PRC activity is not criminal and its technology transfer regime is a threat to U.S. national security, then lawmakers must examine whether current laws and regulations, including export controls, should be modernized.

Export Controls as a Strategic Asset

Because export control officials can approve or deny the transfer of U.S.-origin items to China, it can be a “strategic asset”—as referred to by National Security Advisor Jake Sullivan—to deprive General Secretary Xi of the technology he needs to build a more lethal military and sophisticated surveillance state. Through the bipartisan *Export Control Reform Act of 2018* (ECRA) and recent legislative updates, Congress has given BIS tremendous authority to stop, or at least slow down, technology diversion to the CCP’s military or surveillance state.


Despite Congress passing ECRA and empowering BIS to draft new regulations to address unique features of China’s economy, including MCF, the bureau has not aggressively or proactively done so.^{xxx} Rather, it is maintaining a reactive approach, generally responding only after a crisis occurs.



For instance, export controls on advanced semiconductors and supercomputers were put in place only after discovering the use of U.S. technology in the development of the PRC's hypersonic weapons.^{xxxix} Furthermore, Tianjin Phytium Information Technology, a Chinese supercomputing firm found to have been involved in PRC weapons of mass destruction (WMD) programs was put on the BIS entity list, which restricts its access to U.S. technology, only after the *Washington Post* published an expose about the export control failure. Since enactment of ECRA, the BIS-administered export control system failed to stop the transfer of U.S. semiconductor technology used in the development of the PRC's hypersonics weapons program.^{xxxix} BIS has also failed to stop a PRC state-owned institute from importing Intel and Nvidia chips from the United States for use in China's top nuclear-weapons lab.^{xxxix} It twice failed to prevent the use of Thermo Fisher Scientific DNA equipment from being used in Xinjiang.^{xxxix xxxv}

In addition to reported failures, BIS has not implemented key portions of ECRA, including identifying emerging and foundational technology and reviewing license requirements through the lens of MCF.^{xxxix} A statutory requirement in ECRA Section 1759 to review controlled items based on MCF apparently achieved nothing, because no new controls have been issued. A statutory requirement in ECRA 1758 to identify emerging and foundational technology has resulted in zero foundational technology controls.

Some former officials credit these failures more to culture and mindset than lack of authority or resources. Former Deputy National Security Advisor Matt Pottinger said BIS, "has struggled to reconcile its mission to protect U.S. national security with the Commerce Department's objective of promoting U.S. exports. The dilemma is most acute when it comes to China."^{xxxix}



Former Acting Under Secretary Nikakhtar believes BIS “view(s) itself more as an export promotion agency rather than a national security regulatory body.”^{xxxviii} Numerous current and former officers told HFAC majority staff that BIS struggles to achieve its national security mission because it sits within the Department of Commerce, which is designed to increase exports.

The observed failures over several years prompted Chairman McCaul to examine BIS more thoroughly and identify areas for further actions, including enhanced oversight and legislation. Following this intensive review, Chairman McCaul has concluded that the export control regime must evolve on two simultaneous tracks.

First, BIS’ current organizational structure and policies no longer work. The bureau needs major reforming to ensure the national security mission is not undermined by countervailing goals—such as export promotion.

Second, the export control regime needs immediate modernizations to limit, and ideally stop, the hemorrhaging of sensitive U.S. technology to China. The main, immediate efforts include:

- Enhancing Equity on the Operating Committee
- Modernizing Licensing Policy for China
- Updating Entity List and End-use Check Requirements
- Reinvigorating Plurilateral Export Controls
- Strengthening End-Use Checks and Enforcement
- Issuing New Controls on Fundamental Research
- Improving Congress’ Ability to Do Oversight




ENHANCED EQUITY ON THE OPERATING COMMITTEE

Operating Committee Structure and Process

The Bureau of Industry and Security’s Office of Export Administration reviews license applications subject to the Export Administration Regulation (EAR)—the regulatory authority that implements the requirements in ECRA. The Departments of Defense, Energy, and State have the authority to review and offer recommendations on any license application submitted under the EAR.^{xxxix} Before BIS approves or denies a license, it can conduct a check to establish the identity and reliability of the recipient of licensed items.^{xi} In instances where the reviewing agencies are not in agreement on whether to approve or deny a license, the license is escalated to the Operating Committee.^{xli}

The Operating Committee is chaired by a career employee of BIS—who is meant to be an impartial decision-maker—and it consists of representatives from the Departments of Defense, State, Energy, and Commerce.^{xlii} (The individuals staffing the Operating Committee are career civil servants.) The members can offer advisory opinions to the Chair (BIS) about an application, but the Chair makes the final decision—except for cases involving jet engine hot section technology and commercial communications satellites which can be decided by majority vote.^{xliii} If any agency disagrees with the Chair’s decision, the agency may appeal the decision by requiring the Advisory Committee on Export Policy (ACEP) to vote on the license determination within five days of the Operating Committee Chair’s written decision, or the decision is final.^{xliv}



BIS's Assistant Secretary of Export Administration chairs the ACEP. The ACEP is comprised of assistant secretary-level officials from the same four departments as represented in the Operating Committee, plus the intelligence community. Unlike the Operating Committee, all outcomes at the ACEP are based on majority vote (i.e. one vote per member).^{xlv} If any agency disagrees with the ACEP's decision, the agency may escalate the decision to the Export Advisory Review Board (EARB).^{xlvi}

The Secretary of Commerce chairs the EARB. The EARB is comprised of cabinet-level officials from the same four departments. All outcomes are based on majority vote.^{xlvii} If any agency disagrees with the EARB's decision, the agency may escalate the decision to the President.

The current Operating Committee process imposes strict timelines for elevation of licenses to the ACEP and the EARB—described more below.^{xlviii} Those timelines were developed at a time, however, when license applications were not as complicated as they are today.^{xlix} The intra-governmental documentation needed for escalation of an application to the ACEP, the EARB, or even the President, is extensive.ⁱ Without adequate time to conduct a detailed analysis of the questions related to a complicated license application, Operating Committee member agencies may be unable to raise concerns to the ACEP, the EARB, or the President because analyses may not be completed within the prescribed timelines.ⁱⁱ Practically, because these time limitations inhibit the significant analytical work required to overcome the Chair's decision, it negates any perceived fairness in the escalation process, minimizes the equities of the other national security agencies, and resembles the timelines of a bygone era.ⁱⁱⁱ



In practice, few licenses are escalated to higher decision-making bodies. Of the more than 41,000 license applications BIS processed in fiscal year 2021, less than one percent were escalated to the Operating Committee.^{liii} Because the Operating Committee, unlike the ACEP and the EARB, is not required to make decisions by majority vote in most cases, it can reach non-consensus outcomes.

Statistics provided by BIS of the Operating Committee for fiscal years 2017-2019 show that there has been a 60 percent increase in non-consensus decisions during that time. More than 10 percent of the time, it appears the Operating Committee Chair (BIS) took a position that only one Operating Committee member supported. Because the Department of Commerce is both the Chair and a member, the data raise concerns that Commerce may be abusing its position as the final, only vote on the Operating Committee to override the objections of other agencies.

FY 2017

- 336 licenses were escalated to the OC.
- 112 OC decisions were made without interagency consensus.
 - 66 were approved and 46 were denied.
- 18 of these decisions did not reflect the interagency majority.
- 17 were escalated to the ACEP.

EXPORT ADVISORY REVIEW BOARD



Five days
to
escalate

ADVISORY COMMITTEE ON EXPORT POLICY



Five days
to
escalate

OPERATING COMMITTEE



FY 2018

- 326 licenses were escalated to the OC.
- 121 OC decisions were made without interagency consensus.
 - 66 were approved, 48 were denied, and 6 were returned without action.
- 19 of these decisions did not reflect the interagency majority.
- 26 were escalated to the ACEP.

FY 2019

- 380 licenses were escalated to the OC.
- 179 OC decisions were made without interagency consensus.
 - 123 were approved, 47 were denied, and 9 were returned without action.
- 23 of these decisions did not reflect interagency majority.
- 18 were escalated to the ACEP.

Steve Coonen, who spent nearly 14 years as an analyst for the Defense Technology Security Administration at the Department of Defense, recommends a majority vote process for all licenses before the Operating Committee. He suggests a majority vote for a denial should be the Operating Committee's final disposition, with no prospect for elevating the decision to the ACEP.^{liv} In the event of a two-to-two tie vote, Mr. Coonen says the license should be denied.^{lv}



As mentioned above, ECRA states that the Operating Committee can take a majority vote for certain technologies. Although ECRA does not explain the rationale for taking a majority vote for these two items, it may be because these items were previously on the U.S. Munitions List, overseen by the State Department, and therefore more critical to national security. It is reasonable to conclude that other types of technologies or exports to certain adversaries, which could adversely affect national security, should also be decided by majority vote. Again, it is important to stress, the Operating Committee is the only adjudication body for licenses that does not use a majority vote system.


Problem: The Operating Committee is minimizing the equities of national security agencies in adjudicating licenses.

Recommendation: The Operating Committee should use a majority vote system for all licenses it reviews.

MODERNIZED LICENSING POLICY FOR CHINA

Export Control Classification

In addition to controlling the license adjudication process, BIS is also responsible for determining whether a license is required to export a technology. This process is referred to as a commodity classification.^{lvi} Although BIS is required to request input from certain interagency officials on whether an item is controlled (i.e. whether it falls under a specific Export Control Classification Number),^{lvii} BIS officials routinely ignore their recommendations, according to officials familiar with the process.^{lviii}



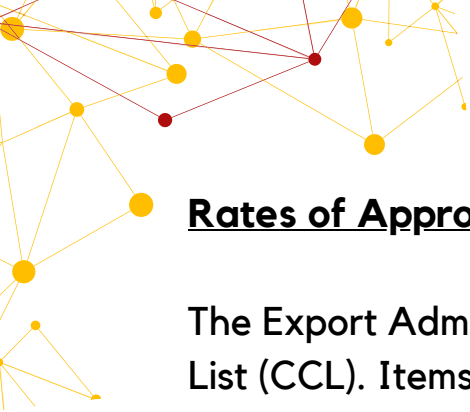
There is also no dispute resolution mechanism for disagreements about how BIS classifies an item.^{lix} Simply put, BIS is the only arbiter in deciding what is and what is not controlled.^{lx}

This matters because BIS can unilaterally decide that a technology does not require a license because it is EAR99—which is a term for any item not on the Commerce Control List—or falls under a license exception or No License Required for a controlled item. “No License Required” is a shipment designation that can be used for either EAR99 items or items on the Commerce Control List that do not require a license for their destination, end use, or end-user.^{lxi} If BIS makes unilateral technology classifications, other agencies that may have concerns about a technology being transferred to a specific end-user or end-use might never have an opportunity to provide input from their subject matter experts.

Considering interviews with current and former licensing officials that expressed frustration with both the commodity classification and the license application review process (15 CFR § 750.3), HFAC majority staff are concerned BIS is not giving full, or any, consideration to other agencies.

Problem: It appears BIS is not following its own regulations, as described in 15 CFR § 750.3.

Recommendation: Mandate BIS refer license applications to other appropriate agencies, including Defense, Energy, and State, for items that implicate their interests (e.g. Defense reviews items controlled for national security and Energy reviews items controlled for nuclear non-proliferation).




Rates of Approval

The Export Administration Regulation contains the Commerce Control List (CCL). Items on the CCL can be controlled for a variety of reasons, including national security, regional stability, nuclear nonproliferation, missile technology, anti-terrorism, and crime control.^{lxii}

All items on the CCL could have a military use, and generally require a BIS license before being exported from the United States. Nonetheless, many items on the CCL are exported under a license exception or a “No License Required” designation. In 2020, nearly 98 percent of CCL items exported to China went without a license.^{lxiii} Even when a license is required, data indicate that BIS almost never denies it. In 2020, BIS denied 2 percent of licenses for U.S. software and technology exports to the PRC and less than 1 percent of licenses to release U.S.-controlled technology and know-how to PRC nationals.^{lxiv} In 2021, BIS approved nearly 90 percent of applications for the export of CCL items to China.^{lxv}

Technologies that “make a significant contribution to the military potential” of a country are controlled on the CCL for national security reasons.^{lxvi} As of August 2021, U.S. government statistics on U.S. exports to China revealed that the U.S. government was approving more than 95 percent of national security-controlled technology transfer requests.^{lxvii} Section 742.4 of the EAR provides a “general policy of approval” for technologies being obtained by Chinese end-users claiming civilian status, as lawful under Section 742.4(b)(7)(i) of the EAR.^{lxviii} As a result, the current policy on national security controls has likely had minimal impact.^{lxix}



In 2021, the value of U.S. licensed controlled exports to China was \$1.5 billion, around 1 percent of total U.S. exports to China.^{lxx} Denying the value of these exports entirely would hardly affect the overall U.S.-China trade relationship or the United States' \$23 trillion economy, but it would better support U.S. national security and blunt CCP military ambitions.^{lxxi}

Nazak Nikhaktar and Steve Coonen both recommend that BIS adopt a “policy of denial” or “presumption of denial” license review standard for all licenses to export items controlled for national security reasons to China.

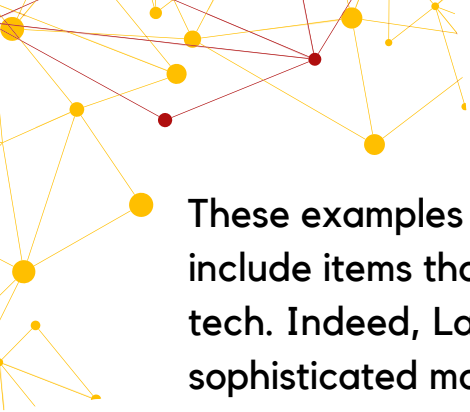
Problem: BIS is approving a large number of items on the Commerce Control List for national security reasons to China.

Recommendation: BIS should impose a “policy of denial” for all exports of national security-controlled items to China.

EAR 99

Items not listed on the CCL are referred to as EAR99. Although BIS refers to these items as “low-technology consumer goods,”^{lxxii} EAR99 items can be high-tech and militarily useful. For example, prior to the recent October 7, 2022 export controls on AI semiconductors, graphic processor units—a type of semiconductor—BIS had no export controls for these items to China.^{lxxiii} Also, weapons used in Russia’s invasion of Ukraine contain a long list of EAR99 components.^{lxxiv}

In 2019, EAR99 was the second highest denied category for exports to China,^{lxxv} and EAR99 was the most denied category for exports to PRC companies on the Entity List from January 2, 2022 to March 31, 2022.^{lxxvi} Furthermore, all emerging and foundational technologies that have not been designated on the CCL are by definition EAR99.



These examples highlight that the EAR99 category does, in fact, include items that are sensitive and are certainly not uniformly low-tech. Indeed, Lam Research, which makes some of the world's most sophisticated machines to manufacture semiconductors, told an investor conference in 2020, "We don't need any licenses as we sit here today to sell anything in China."^{lxxvii} It is clearly misleading for BIS to refer to EAR99 as purely "low-level."^{lxxviii}

The use of EAR99 technology to support the militaries of U.S. adversaries makes the appearance of limited action tied to Section 1759 of ECRA so alarming. Considering the aims of MCF and General Secretary Xi's goal to have a military capable of invading Taiwan by 2027, BIS must more aggressively identify and control items currently classified as EAR99.

Problem: Sensitive, militarily useful items remain designated EAR99, and therefore are not subject to any licensing requirement for transfers to China.

Recommendation: BIS must seriously review EAR99 technologies and control or re-control items on the Commerce Control List.

UPDATED ENTITY LIST REQUIREMENTS

End-Use and End-User Controls

In addition to technology controls through the CCL, BIS can use end-use and end-user controls to deny technology transfers to a specific company or individual. These controls include designation on the Entity List, a list subject to specific license requirements for export, reexport, and/or transfer of specific items.^{lxxxix} The legal requirement to be designated on the Entity List is broad—i.e. entities acting or at significant risk of acting contrary to the national security or foreign policy interests of the United States.^{lxxx} Companies on the Entity List are typically subject to a presumption of denial for items subject to the EAR. In recent years, BIS has begun applying a presumption of denial only for select items. For instance, Huawei’s licensing policy is a presumption of denial only for items capable of supporting 5G. And, originally, SMIC was subject to a presumption of denial only for items uniquely required to produce semiconductors at or below 10 nanometers.

Problem: BIS is using a licensing regime that allows companies on the Entity List to access large swaths of technology either without a license or under a presumption of approval.

Recommendation: BIS should apply a presumption of denial for all items subject to the EAR for companies on the Entity List.

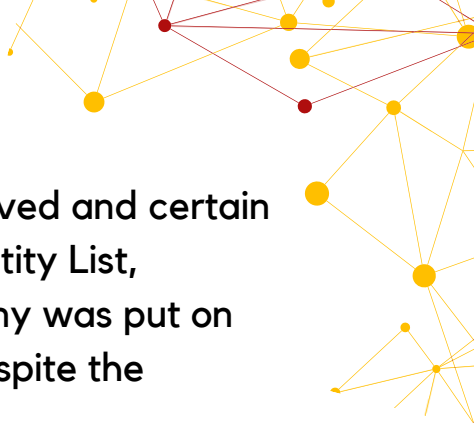


The Entity List

The End-User Review Committee (ERC) is an interagency body chaired by the Department of Commerce and comprised of representatives from the Departments of Commerce, Defense, State, and Energy that reviews additions and removals of parties on the Entity List.^{lxxxix} A majority vote is required to add an entity to the Entity List, and a unanimous vote is required to remove or modify an entry.^{lxxxii} Only the Chair can bring an Entity Listing to a vote by the other agencies. Entities on the Entity List are typically subject to a presumption of denial licensing policy for all items subject to the EAR. Nevertheless, license applications for companies on the Entity List do not appear to be overwhelmingly denied—in fact it appears the opposite is happening:

- During a six-month period between November 2020 and April 2021, BIS approved \$60 billion worth of licenses for Huawei and \$40 billion worth of licenses for SMIC.^{lxxxiii}
- During a three-month period between January and March 2022, BIS approved more than \$23 billion worth of licenses and denied only 8 percent of license applications for PRC companies on the Entity List.^{lxxxiv}

Neither the Export Control Reform Act nor the Export Administration Regulations define what a “presumption of denial” means. House Foreign Affairs Committee majority staff have been informed about discussions for granting licenses to companies on the Entity List. In one instance, Commerce and Defense argued that, because an export of a controlled technology to a company carrying out the Chinese Communist Party’s genocide in Xinjiang was not linked to the reason for the company being placed on the Entity List, the export should be allowed.



State expressed concern about the license being approved and certain information being transferred to the company on the Entity List, regardless if it was connected to the reason the company was put on the Entity List. Ultimately, the license was approved, despite the “presumption of denial.”

Problem: Without a clear definition and criteria, each agency possesses a subjective standard of determination by which Congress is unable to hold the Commerce Department to account.

Recommendation: “Presumption of denial” should be defined to mean a license, no matter the item, will be denied essentially in every instance. BIS should state this clearly in its regulations, otherwise Congress should write it into law.

The Entity List is meant to be a flexible tool that can be used quickly. The low threshold for designation means BIS takes on limited legal risk. It has been referred to as the “I don’t like your face” standard—referring to the ease and minimal risk associated with an Entity Listing.

The Department of Commerce has prevailed twice in recent court cases initiated by PRC companies regarding their Entity List designations. In one example, the U.S. District Court for the District of Columbia affirmed in *Chanji Esquel Textile Co. LTD., et al v. Gina Raimondo* that “the ECRA precludes this Court from engaging in such an APA [Administrative Procedures Act] review.”^{lxxxv} Because Congress, through ECRA,^{lxxxvi} exempted the Entity List from the *Administrative Procedures Act*—which puts more burden on the government to show that an action is not arbitrary or capricious—parties have struggled significantly to challenge Entity List designations. HFAC majority staff are unaware of any instance in which a PRC company prevailed over the U.S. government in court with respect to an entity listing.



Ineffective Use of the Entity List by BIS

The Entity List should be an effective tool to cut off a company from U.S. technology, but is too often used in a piecemeal way. Unlike the Department of the Treasury Office of Foreign Asset Control's 50 Percent Rule,^{lxxxvii} BIS typically designates a specific affiliate of a company instead of the entire corporate structure, including subsidiaries and affiliates. In the case of SenseTime—a PRC company selling AI surveillance equipment to oppress Uighurs—the company told investors “the Entity List Addition has not had any material adverse impact on our business.”^{lxxxviii} An attorney for SenseTime concluded that only Beijing SenseTime, and no other parts of the organization, was restricted from doing business with U.S. firms.”^{lxxxix} In a similar example, following its designation on the Entity List, Inspur Group—a PRC server manufacturer found to have been doing business with the PLA—received assurances that some U.S. companies reportedly planned “to continue shipping goods to Inspur’s subsidiaries barring any guidance contrary from Commerce.”^{xc} Significant portions of Beijing Genomics Institute, a national champion for the CCP’s global biotechnology sector, remain unlisted despite the company being a risk for “diversion to China’s military programs.”^{xc1} Former BIS officials told HFAC majority staff that identifying one subsidiary at a time, “ignores the reality that the entire corporate system in the People’s Republic of China (“PRC”) is encouraged—and often mandated—by the PRC government to circumvent U.S. laws.”^{xcii}

In addition to missing large parts of an entity’s corporate network, BIS is also not designating large swaths of the PRC military and surveillance ecosystem. The Center for Security and Emerging Technology found that of the 273 PLA AI equipment suppliers identified in its 2021 study, just 8 percent are named in U.S. export control and sanctions regimes.^{xciii}



Kharon, a Washington, D.C.-based research and data-analytics firm, said it has identified tens of thousands of Chinese entities that may meet the U.S. criteria for military end-user export restrictions.^{xciv} Indeed, numerous companies exist that have software to identify Chinese military companies and their subsidiaries and affiliates instantly.

Following more restrictive export controls, Huawei—added to the Entity List in May 2019^{xcv}—sold Honor, its 5G business, to the PRC government.^{xcvi} Chairman McCaul and members of the China Task Force called on Secretary Raimondo to designate Honor on the Entity List.^{xcvii} Senators Rubio, Scott, and Cornyn also urged the Biden administration to list Honor.^{xcviii} The Congressional Research Service used Honor as an example of “Chinese companies...restructuring themselves potentially to circumvent U.S. export and investment restrictions.”^{xcix} To date, Honor is not on the Entity List. PRC companies on the Entity List are finding novel ways to evade export restrictions. iFlytek and SenseTime, both on the Entity List for supporting Beijing’s genocide in Xinjiang, are reportedly using cloud providers and rental agreements with third parties, as well as purchasing controlled semiconductors through subsidiary companies to access high-end U.S. technology.^c This means companies that should be prohibited from using advanced semiconductors have found a loophole in the rules to maintain their access to these chips—which have been used to abuse human rights.

Yangtze Memory Technologies Corp (YMTC)—the PRC’s top state-owned memory chip maker—reveals the paralysis in the Entity Listing process. In 2021, Chairman McCaul wrote a letter to Secretary Raimondo urging her to designate YMTC on the Entity List.^{ci} Chairman McCaul pressed Secretary Blinken about YMTC at a House Foreign Affairs Committee hearing later that year; Secretary Blinken appeared unaware of the company.



In a subsequent House Foreign Affairs Committee hearing, Chairman McCaul displayed visual proof (i.e. a YMTC chip in a Huawei phone) to BIS Under Secretary Estevez that YMTC was violating export controls on Huawei, which can be a basis for being designated on the Entity List. In 2022, the Biden administration finally designated YMTC on the Entity List. In total, it took nearly two years for BIS to take an action that needed only the stroke of a pen.

Problem: The Entity List is not reflecting the scope of military end-users or entities that threaten or have the potential to threaten U.S. national security or foreign policy interests.


Recommendations: The entire corporate network of listed companies should be incorporated in each Entity List designation; at the very least, BIS should adopt OFAC's 50 percent rule when listing a company.

BIS must invest in existing, commercially available software and databases that identify PRC companies and subsidiaries with links to the CCP's military.

The provision of cloud services should be a licensable activity and prohibited to companies on the Entity List.

Military End-user Rule

The Trump administration revised two BIS end-use rules to address the CCP's Military-Civil Fusion strategy. The Military End-User (MEU) rule establishes a licensing requirement for exporters who knowingly send a specific sub-set of controlled items to military end-users in China.^{cii} No license is required to export EAR99 or items on the CCL not specifically identified in the rule to a MEU in China.



The MEU rule for China is less restrictive than the MEU rule for Russia. For Russia, the MEU rule prohibits transfers of all items subject to the EAR (i.e. both EAR99 and CCL) to military end-users. The MEU rule for China allows unlicensed transactions for EAR99 and sections of the CCL not specifically referenced in the rule.

Moreover, BIS takes a narrow definition of a “military end-user.” Section 744.21(g) of the Export Administration Regulation defines a military end-user as:

“...[T]he national armed services (army, navy, marine, air force, or coast guard), as well as the national guard and national police, government intelligence or reconnaissance organizations (excluding those described in § 744.22(f)(2)), or any person or entity whose actions or functions are intended to support ‘military end-uses’...”

This definition covers only a subset of companies that are carrying out the CCP’s MCF strategy. Congress, through Section 1260H of FY2021 *National Defense Authorization Act*, provided a more robust, comprehensive definition for a Chinese military company.^{ciii} Specifically, it includes a definition for “Military-civil fusion contributor” to cover notionally private companies that are supporting the military.^{civ} The narrow definition in Section 744.21 may account for the low number (71) of PRC entities on the MEU list, considering the expansive nature of MCF.

Problem: The executive branch is not using a standard definition of a Chinese military company.

Recommendation: BIS should adopt concepts in the 1260H definition for its definition of MEU, and Congress should be prepared to legislate this definition if BIS is unwilling to do it.




REINVIGORATED PLURILATERAL CONTROLS

The Wassenaar Arrangement is the current multilateral regime coordinating international dual-use export controls. Established at the end of the Cold War, Wassenaar has existed for nearly 30 years. Unfortunately, Wassenaar has been unable to constrain the rise of the CCP's military and surveillance state. Indeed, China's use of surveillance technology to carry out a genocide and its hypersonic test^{cvi} gives greater urgency to reexamining the efficacy of the existing system and considering new approaches around specific emerging and foundational technologies.

The Wassenaar Arrangement is a multilateral body consisting of 42 countries, including Russia, that controls dual-use technologies and munitions. The Wassenaar List of controlled technologies is the foundation for the U.S. Commerce Control List as well as the control lists for allied and partner countries. Because Wassenaar is a consensus-based body, one dissenting member can veto a proposal to control a technology. At the December 2022 Plenary Session of the Wassenaar Arrangement "little more than a few grammatical changes" were made and former Assistant Secretary of BIS under the Obama administration, Kevin Wolf, guessed that "the Russian delegation vetoed all material changes."^{cvii} Wassenaar is exposing the shortcomings in large, multilateral bodies that require consensus to control new technologies.

Wassenaar also suffers from national licensing discretion for controlled items. Although member countries may agree to control all the items on the Wassenaar List, each member country can set its own licensing policy for that item.



For example, BIS may deny a license to an American exporter to transfer controlled technology to China, but another member country may approve a license from one of its exporters to transfer the same or similar technology to China. This framework creates meaningful gaps that could harm U.S. national security interests and that of our allies.

The Trump and Biden administrations have begun pursuing unilateral controls alongside bilateral and plurilateral agreements. During the Trump administration, Secretary Pompeo reportedly directly lobbied the Dutch government to restrict sales of certain semiconductor manufacturing equipment to China.^{cviii} In January 2023, the United States, the Netherlands, and Japan reached a deal to align export controls on advanced semiconductor equipment to restrict the PRC's development of high-end, advanced semiconductors.^{cix}

The move toward binding bilateral or plurilateral agreements is rooted in U.S. export control history. During the Cold War the United States and a several allies created the Coordinating Committee for Multilateral Export Controls (CoCom) to restrict technology exports to the USSR. Unlike the Wassenaar Arrangement, which is geopolitically neutral, CoCom targeted a shared adversary—Soviet Russia.^{cx} Each member had the ability to stop another country from exporting a controlled technology to the USSR.



Problem: The multilateral regime for export controls is incapable of achieving meaningful control on technology transfers to the PRC.

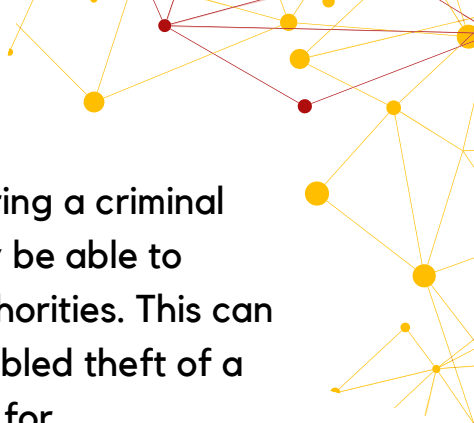
Recommendation: The United States must continue its push for bilateral and plurilateral agreements. Ideally, these agreements should result in adopting the same legal and regulatory requirements within their respective countries to control specific emerging or foundational technology. In addition to semiconductors, the U.S. government must, at a minimum, pursue agreements on AI, quantum, and biotechnology in the near-term along with our allies.

STRENGTHENED END-USE CHECKS, ENFORCEMENT, AND OVERSIGHT

BIS is the only export control agency in the world with their own enforcement authority. The Office of Export Enforcement's responsibilities include investigating export and antiboycott violations, interdicting illegal exports, conducting end-use checks, and initiating criminal prosecutions or administrative enforcement actions.

BIS also has an array of partnerships and memorandums of understanding (MOU) with other law enforcement and intelligence agencies across the federal government. This includes the Disruptive Technology Strike Force, a partnership between the Departments of Commerce and Justice designed to enhance BIS enforcement and prosecution capabilities.^{cx1}

Partnerships like the Disruptive Technology Strike Force provide BIS export enforcement with additional tools and opportunities for criminal prosecutions or administrative actions.



For instance, if the Department of Justice is not able to bring a criminal charge under its authorities, BIS export enforcement may be able to pursue an administrative penalty using export control authorities. This can be particularly effective for instances in which cyber-enabled theft of a controlled technology may allow BIS to use its authorities for administrative penalties.

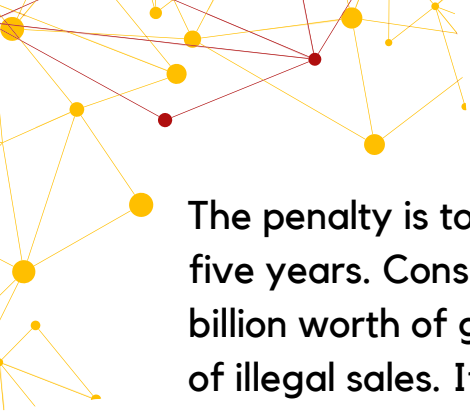
Nonetheless, the Office of Export Enforcement struggles to get criminal prosecutions due a statutory requirement to prove “willfulness.”^{cxii} This high bar often results in BIS export enforcement personnel pursuing administrative enforcement actions with lower penalties.

Problem: The “willfulness” standard for criminal prosecutions appears nearly insurmountable to reach.

Recommendation: Congress should legislate a new standard for criminal prosecutions to support enforcement actions that deter future evasion or violations.

Recent Actions and Investigations

BIS enforcement actions have at times been slow. Seagate Technology—a mass data storage company—provides an instructive example. In September 2020, Seagate said it continued to sell hard drives to Huawei and did not believe it needed a BIS license, despite its competitor, Western Digital, pausing all shipments to Huawei.^{cxiii} In October 2021, the Senate Committee on Commerce, Science, & Transportation issued a report alleging that Seagate violated export controls prohibiting shipment to Huawei.^{cxiv} Nearly a full year later, on August 29, 2022, Seagate disclosed in SEC filings that it received a proposed charging letter from BIS alleging violations of the Export Administration Regulations.^{cxv} In April 2023, BIS at last imposed a \$300 million administrative penalty against Seagate.^{cxvi}




The penalty is to be paid in installments of \$15 million per quarter over five years. Considering Seagate illegally sold Huawei more than \$1 billion worth of goods, a \$300 million penalty is a fraction of the amount of illegal sales. It is unclear if this action will change the industry's behavior. Some observers told HFAC majority staff that the low fine may give an incentive to break rules, risk getting caught, and try to negotiate a weaker monetary penalty. Other observers stated that the complexity of new export control rules makes investigations and prosecutions much more difficult.

In April 2022, Bloomberg reported that Synopsys Inc., the biggest U.S. supplier of software used to design semiconductors, was under investigation by BIS for violating export controls on shipments to SMIC and Huawei.^{cxvii} Specifically, that Synopsys had been providing chip designs and software to the aforementioned PRC parties. To date, it does not appear BIS has taken any action against Synopsys. Meanwhile Huawei has reemerged as a serious contender in 5G and SMIC is producing 7nm chips—advanced technology for semiconductors that had been only capable of development by TSMC, Intel, and Samsung. Despite this breakthrough by SMIC, which almost certainly required the use of U.S. origin technology and should be an export control violation, BIS has not acted.

End-Use Checks

BIS' export enforcement personnel are responsible for conducting site visits, also known as end-use checks involving items subject to the Export Administration Regulations, to verify compliance. BIS uses end-use checks to confirm the legitimacy and reliability relating to an end-use or end-user and to monitor an end-user's compliance with the terms of its license.



End-use checks in China are conducted pursuant to a 2004 classified agreement between the U.S. and PRC government. The bilateral end-use check agreement permits only one full-time Export Control Officer (ECO) to conduct pre-license checks (PLC) and post-shipment verifications (PSV) inside China.^{cxviii} With other countries, U.S. export control officers can conduct end-use checks with few restrictions for up to five years after a technology is shipped.^{cxix} But, unique to the PRC, U.S. officials have only 180 days after an item is shipped to submit a request to conduct an end-use check.^{cxviii} Additionally, even with this agreement in place, the PRC would still need to accept a U.S. government request to conduct an end-use check.^{cxx} In data obtained by HFAC majority staff, from the time the request is made to the date an inspection is conducted can take more than 100 days. To prevent the concealment of violations, it is essential that end-use checks are conducted immediately—ideally within 24 hours—of a request.

Between 2016 and 2021, the United States government's two export control officers in China conducted on average only 55 end-user checks per year of the roughly 4,000 active licenses in the PRC.^{cxxi} Put another way, BIS likely verified less than 1.5 percent of all licenses, which represent less than one percent of all trade with the PRC. Steve Coonen, a former DoD export control official said the agreement "serves as an invitation for diversion rather than its intended purpose of dissuasion." Mr. Coonen argues that the agreement should be renegotiated because "it affords the U.S. no effective means to confirm actual end-use or end-users in China."^{cxviii} Moreover, it is increasingly challenging to conduct any due diligence in the PRC. In recent months, PRC authorities have restricted or cut off overseas access to databases involving corporate-registration information.^{cxviii} Additionally in March 2023, PRC authorities raided the U.S. corporate due diligence firm Mintz Group without explanation, detaining five local staff and closing its China operations.^{cxviii}




The crackdown has extended to forced labor, as PRC security forces raided the U.S. labor rights nonprofit Verite Inc.^{cxxv} The Big Four auditing giants—PricewaterhouseCoopers (PwC), Deloitte, KPMG International Limited (KPMG), and Ernst & Young (EY)—have all shut down their legal affiliations in the PRC following “intense regulatory scrutiny.”^{cxxvi} PRC authorities have also urged State-Owned Enterprises to drop the big four auditors. In fact, as a result of U.S. think tank reports related to export controls, Beijing shut down access to many open-source data bases.^{cxxviii}

Problem: The end-use check agreement severely limits BIS’ ability to conduct checks on its own terms and schedules.

Recommendation: The Department of Commerce must renegotiate its end-use agreement with the PRC or impose greater restrictions on exports to China considering the inability to conduct meaningful end-use checks.

Transparency

Additional access to licensing decisions is needed to conduct oversight of BIS. This data helps Congress understand where BIS is drawing the line on national security and whether BIS is carrying out license decisions on a level playing field. For example, there is ongoing speculation that Qualcomm has been the only company that has received a license to sell 4G chips to Huawei, giving it a *de facto* monopoly.^{cxxvix} In fact, Qualcomm’s CEO has said, “To date, we have not been impacted by any restrictions.”^{cxxx} Only through transparency on discrete licensing decisions can Congress parse rumor from fact. Moreover, with greater transparency on the specific items being labeled as EAR99, Congress can better understand the types of technologies that are in this category.



Regrettably, BIS cooperation with HFAC, pursuant to its statutory requirements in the *Export Control Reform Act*, has been unsatisfactory. In November 2020, then-Ranking Member McCaul requested information on all BIS licensing decisions for PRC companies on the Entity List with reoccurring updates. More than six months later, in May 2021, BIS provided then-Ranking Member McCaul with an incomplete tranche of documents that included licensing data for only SMIC and Huawei. It then took BIS more than 18 months, on January 31, 2023, to provide Chairman McCaul with a second tranche of data. All data should have been provided by the May 2021 date; this lack of transparency and efficiency is extremely troubling.

Problem: Despite ECRA giving the Chair or Ranking Member of a Committee of jurisdiction authority to receive licensing information, BIS is either slow to provide or withholds information that is needed to conduct basic oversight.

Recommendation: Congress should amend ECRA to require regular reports on licensing decisions for companies on the Entity List.

New Policies on Fundamental Research

Fundamental research is critical to the U.S. innovation enterprise. Current U.S. government policy regarding fundamental research is based on National Security Directive (NSD) 189—developed in 1985 by the Reagan administration.^{cxxxix} NSD 189 was developed in response to “the acquisition of advanced technology from the United States by Eastern Bloc nations for the purpose of enhancing their military capabilities.”^{cxxxix} A 1982 National Academy of Sciences study concluded that fundamental research was a “minor contributor” to technology transfer to the Soviet Union.

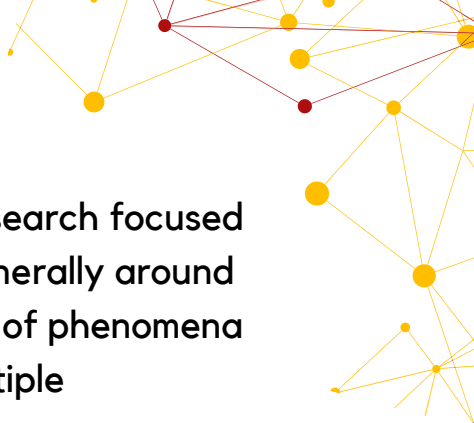


As a result, NSD-189 set a policy that “the products of fundamental research remain unrestricted.”^{cxxxiii} It is safe to say that the directive needs to be updated to reflect two generations of strategic shifts.

Each year the PRC steals upwards of \$600 billion worth of American intellectual property.^{cxxxiv} Director Wray of the Federal Bureau of Investigations stated recently that, “When we tally up what we see in our investigations—over 2,000 of which are focused on the Chinese government trying to steal our information or technology—there is just no country that presents a broader threat to our ideas, our innovation, and our economic security than China.”^{cxxxv}

In May 2022, it was reported that the National Science Foundation (NSF) was indirectly funding research involving a PRC entity on the Entity List. A senior official at NSF said the U.S. awardee told NSF that the grant was legal because “this is fundamental research and so the Entity List doesn’t apply here.”^{cxxxvi} HFAC majority staff understands that the PRC entity was involved in the PRC’s genocide of ethnic Uighurs. Former Acting Under Secretary Nikakhtar contends that the possibility that research may be published in the future should not be a sufficient reason for exempting that research from controls today.^{cxxxvii} It appears the fundamental research exception is acting more like a loophole for PRC access to U.S. innovation.

The fundamental research exception remains one of the more inconsistently applied concepts across U.S. export laws.^{cxxxviii} Universities, research institutes, government laboratories and others routinely look to the fundamental research exception in the EAR (§ 734.7) to eliminate export licensing requirements for cross-border activities.^{cxxxix}



At the time the concept was established, fundamental research focused primarily on basic research.^{cxli} Basic research revolves generally around theories and principles common to the foundational study of phenomena or other concepts that are key to the development of multiple applications.^{cxli}

Today, however, the concept includes both basic and application specific research and it is this expansion that has created gaps in the process which allows for more expansive cross-border engagements over which the U.S. government writ large lacks visibility.^{cxlii} Without visibility into the exchanges that occur, the U.S. government is unable to gauge where and how limitations may be needed and thus predicates some of its regulatory decisions on incomplete information.^{cxliii}

Problem: NSD-189 is designed to solve a technology transfer problem from the 1980s and is ineffective with respect to current PRC state-sponsored theft.

Recommendation: NSD-189 must be reformed by the Biden administration to address China's acquisition of critical technology and know-how through fundamental research and Congress must put adequate safeguards on fundamental research.

BIS Resources and Personnel

BIS needs targeted modernizations to better address technology transfers to U.S. adversaries and efforts to evade U.S. law. These issues include: the organization's severely outdated information technology system and a severe lack of subject matter experts and linguists focused on the PRC.^{cxliv} The Center for Strategic and International Studies notes "BIS analysts perform their work primarily using Google searches and Microsoft Excel."^{cxlv}



In an interview with a former BIS official, HFAC majority staff were told the bureau had one employee proficient in Mandarin during their tenure. Additionally, as it relates to general technical expertise, at one point BIS apparently only employed one member of staff who could maintain and operate the Federal Register system, which is needed for any regulatory update.

The Bureau of Industry and Security appears not to have prioritized hiring people with the linguistic, technical, or geopolitical expertise needed to carry out its mission. The Bureau of Industry and Security received a substantial \$22,100,000 within the *Ukraine Supplemental Appropriations Act of 2022* to employ temporary personnel to carry out the increased workload due to the Russian invasion of Ukraine.^{cxlvi} Additionally, within the FY2024 Presidential Budget Request for BIS, the request for funding and resources do not meet nor match the shortcomings BIS needs to effectively carry out their mission.^{cxlvii} BIS has had opportunities to use the resources provided to them to increase the efficacy and efficiency of their work with talented personnel and technological modernization. BIS has also equally had the opportunity to advocate for additional resources to assist in their vital mission. Deputy Assistant Secretary of Commerce for Export Administration Matt Borman has stated, "We spend 100 percent of our time on Russia sanctions, another 100 percent on China and the other 100 percent on everything else."^{cxlviii} However to date, we have not seen improvement nor supplemental requests to improve the linguistic, geopolitical, targeting, and technical expertise of the bureau to address today's threat landscape.

To augment its budget, it was recommended to HFAC majority staff to consider updating ECRA to allow for charging licensing fees to certain designations (e.g. adversarial countries) or end-users (e.g. companies on the Entity List). A modest fee paid for by the license applicant could go toward supporting enforcement efforts.



Problem: BIS argues it is under resourced to carry out its mission.

Recommendation: Amend ECRA to allow BIS to charge fees on certain licenses to support enforcement efforts.

Emerging and Foundational Technology

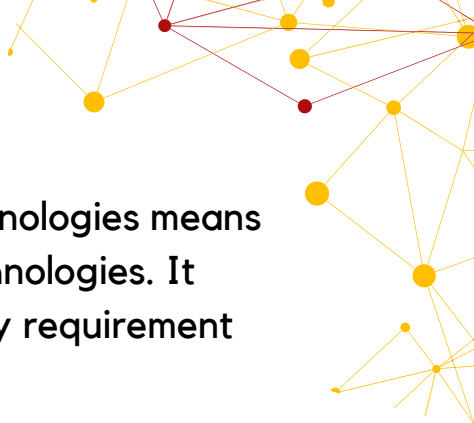
One of the major compromises during the negotiations for the *Foreign Investment Risk Review Modernization Act* and *Export Control Reform Act* (under P.L. 115-232) was the identification and control of emerging and foundational technologies. At the time, Congress was considering giving the Committee on Foreign Investment in the United States (CFIUS) authority to review joint ventures in foreign countries. Ultimately, CFIUS authority over joint ventures was removed in exchange for placing a legal requirement in ECRA Section 1758 to identify and control emerging and foundational technologies.^{cxlvix}

The rationale for controls on emerging and foundational technologies was its clear link to U.S. national security and foreign policy interests. Indeed, the National Counterintelligence and Security Center assesses that emerging technologies may determine a country's status as a superpower.^{cl} A key example being AMD's transfer of state-of-the-art x86 chips, a foundational technology, to Sugon—a PRC supercomputer manufacturer that was subsequently placed on the Entity List in 2019—gave the Chinese Communist Party's military "...the keys to the kingdom" in terms of semiconductor technology.^{cli} Foundational U.S. satellite technology operated by AsiaSat helped the PRC government put down protests in Tibet and Xinjiang.^{clii} Emerging technologies, including artificial intelligence and facial recognition, are enabling genocide in the PRC.^{cliii} Emerging and foundational technologies are inherent to national security, and should not require proving a direct link to a military item.



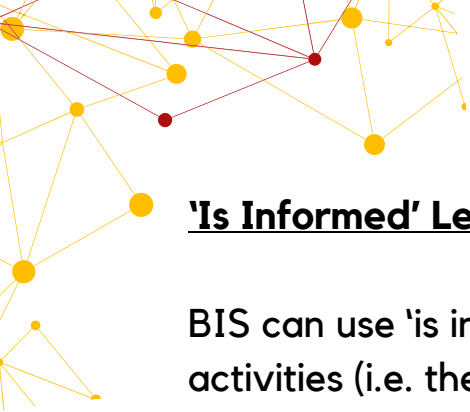
The U.S.-China Economic and Security Commission wrote in 2021 that BIS has failed to implement ECRA's requirements, including on emerging and foundational technology.^{cliv} To date, BIS has identified zero foundational controls. Of the controls on emerging technologies, including for semiconductors and chemical precursors, nearly all of them were controlled through the Wassenaar Arrangement. This process typically takes several years to adopt a control on a technology. By this point, the technology is no longer "emerging" but is now "emerged" and understood. The intent behind ECRA section 1758 was to control items before the U.S. government understood it, and release it, or remove controls, after the U.S. government could mitigate national security concerns related to the technology. Considering the Trump administration^{clv} and the Biden administration^{clvi} both issued a "Critical and Emerging Technologies List," and BIS has issued Advanced Notice for Proposed Rulemaking for Emerging and Foundational technologies in 2018 and 2020 respectively, it is concerning that BIS has been unable to carry out the policy of the White House and the law.

Now, BIS has decided it will no longer label these technologies as "emerging" or "foundational" and instead use the term "1758 technologies." Congress used the "emerging" and "foundational" terms to guide BIS in how to move items from an EAR99 designation to the CCL. The "emerging" term meant brand new technologies never previously designated on the CCL. Whereas the "foundational" term meant items that had been previously moved from the CCL to EAR99 and may require being put back on the CCL.



BIS's failure to identify emerging and foundational technologies means EAR99 no doubt contains sensitive, militarily useful technologies. It further signals that BIS is not approaching this statutory requirement urgently, but rather with a business-as-usual attitude.

Emerging and foundational technology may reveal the inherent conflict of interest with dual-use export controls being under the Department of Commerce. In 2013 the PRC government issued opinions and guidelines on so-called "secure and controllable" technology. At the time, the U.S. business community raised significant concerns that these secure and controllable policies would be used to push U.S. technology companies, including for semiconductors, out of China. In 2014, the PRC government created a \$150 billion fund to build factories to manufacture semiconductors. In 2015, the PRC government issued its Made in China 2025 Plan, which set market share targets for strategic sectors and technologies, including semiconductors, that are to be filled by domestic production.^{clvii} The PRC government was clearly creating a plan to use its market to dominate the semiconductor industry.^{clviii} In 2016, then Commerce Secretary Penny Pritzker said China's semiconductor policy is a "threat to the global semiconductor industry." It is deeply concerning that one year before Secretary Pritzker's speech, BIS removed export controls to China on certain tools, including lithography, used to fabricate semiconductors.^{clix clx} Today, it is estimated that the PRC government outlays to the semiconductor industry reach \$322 billion^{clxi} and \$1.4 trillion in its digital economy.^{clxii} As China is telling the world it intends to take control of the semiconductor industry, BIS is making it easier, when it should be making it harder, to sell China the tools it needs to achieve its goal.



'Is Informed' Letters

BIS can use 'is informed' letters to notify an exporter that certain activities (i.e. the export of a specific technology to a certain country or the transfer of certain technology to a specific entity) may be subject to a license. BIS can use these 'is informed letters' to immediately require a license and potentially deny transfers, without needing to go through a formal Entity Listing or technology control. In theory, these letters could be used to stop the shipment of technology immediately. However, in practice, HFAC majority staff have been told the letters give the appearance of acting without certainty that transfers are in fact being stopped.

There is concern that BIS is using these 'is informed' letters to prevent other agencies from taking more consequential actions. During a recent staff briefing, the Congressional Research Service observed that BIS views the license requirement as the control. Put another way, even though an 'is informed letter' requires a license, the license is likely going to be approved.

HFAC majority staff have been told BIS has also used 'is informed' letters during CFIUS reviews to remove technology controls from National Security Agreements. As a result, CFIUS mitigation agreements leave enforcement of 'is informed letters' to BIS, which sources allege does not share licensing decisions made pursuant to the 'is informed letter' with members of CFIUS. This means CFIUS may aim to block the acquisition of a technology by a PRC company, only for BIS to give the technology to them through a license.



Redefining Standards

In September 2022, BIS issued an interim final rule to authorize the release of items subject to export controls without a license, including to companies on the Entity List, so long as that release occurs in the context of a “standards-related activity.”^{clxiii} Because almost any exchange between two or more entities could be self-classified as a “standards-related activity,” BIS created a dangerous loophole that removes any U.S. government visibility into sensitive technology transfers and undercuts Entity List enforcement.

The U.S. Chamber of Commerce’s submission to the Trump administration’s Section 301 Investigation states that the PRC uses standards to transfer technology. The PRC’s own legal and regulatory regime for standardization “constitute technical barriers to trade and put proprietary information at risk,” according to the U.S. Chamber of Commerce.^{clxv} Consequently, the Biden administration’s rule on standards related activity gives Beijing a path to sidestep export controls, and gain access to sensitive technology.









Problem: BIS has created a loophole that allows China access to potentially sensitive technologies through standard-setting bodies.

Recommendation: BIS or Congress must update the definition for standard-setting organizations to close this loophole.

CONCLUSION

This review illuminates that if the United States wants to effectively address China, then change must occur at BIS. BIS too often puts economic and commercial considerations of single companies before national security. It adopts a piecemeal approach to a comprehensive problem. BIS needs new forward leaning policies that do not measure success in increasing exports or promoting commerce.

APPENDIX I – RECOMMENDATIONS

-  **Problem:** The Operating Committee is minimizing the equities of national security agencies in adjudicating licenses.
-  **Recommendation:** The Operating Committee should use a majority vote system, especially for exports to China.
-  **Problem:** It appears BIS is not following its own regulations, as described in 15 CFR § 750.3.
-  **Recommendation:** Mandate BIS refer license applications to other appropriate agencies, including Defense, Energy, and State, for items that implicate their interests (e.g. Defense reviews items controlled for national security and Energy reviews items controlled for nuclear non-proliferation).
-  **Problem:** BIS appears to be approving a large number of items on the Commerce Control List for national security reasons to China.
-  **Recommendation:** BIS should impose a policy of denial for all exports of national security-controlled items to China.
-  **Problem:** Sensitive, militarily useful items remain designated EAR99, and therefore are not subject to any licensing requirement for transfers to China.
-  **Recommendation:** BIS must seriously review EAR99 technologies and control or re-control items on the Commerce Control List.

Problem: BIS is using a licensing regime that allows companies on the Entity List to access large swaths of technology either without a license or under a presumption of approval.

Recommendation: BIS should apply a "presumption of denial" for all items subject to the EAR for companies on the Entity List.

Problem: Without a clear definition and criteria, each agency possesses a subjective standard of determination by which Congress is unable to hold the Commerce Department to account.

Recommendation: "Presumption of denial" should be defined to mean a license, no matter the item, will be denied essentially every instance. BIS should state this clearly in its regulations, otherwise Congress should write it into law.

Problem: The Entity List is not reflecting the scope of military end-users or entities that threaten or have the potential to threaten U.S. national security or foreign policy interests.

Recommendations:

- The entire corporate network of listed companies should be incorporated in each Entity List designation; at the very least, BIS should adopt OFAC's 50 percent rule when listing a company.
- BIS must invest in existing, commercially available software that identifies PRC companies with links to the CCP's military.
- The provision of cloud services should be a licensable activity and prohibited to companies on the Entity List.

Problem: The executive branch is not using a standard definition of a Chinese military company.

Recommendation: BIS should adopt concepts in the 1260H definition for its definition of MEU.

Problem: The multilateral regime for export controls is incapable of achieving meaningful control on technology transfers to the PRC.

Recommendation: The United States must continue its push for bilateral and plurilateral agreements. Ideally, these agreements should result in adopting the same legal and regulatory requirements within their respective countries to control specific emerging or foundational technology. In addition to semiconductors, the U.S. government must, at a minimum, pursue agreements on AI, quantum, and biotechnology in the near-term along with our allies.

Problem: The “willfulness” standard for criminal prosecutions appears nearly insurmountable to reach.

Recommendation: Congress should develop a new standard for criminal prosecutions to support enforcement actions that deter future evasion or violations.

Problem: The end-use check agreement severely limits BIS’ ability to conduct checks on its own terms and schedules.

Recommendation: The Department of Commerce must renegotiate its end-use agreement with the PRC or impose greater restrictions on exports to China considering the inability to conduct meaningful end-use checks.

Problem: Despite ECRA giving the Chair or Ranking Member of a Committee of jurisdiction authority to receive licensing information, BIS is either slow to provide or withholds information that is needed to conduct basic oversight.

Recommendation: Congress should amend ECRA to require regular reports on licensing decisions for companies on the Entity List.

Problem: NSD-189 is designed to solve a technology transfer problem from the 1980s and is ineffective with respect to PRC state-sponsored theft.

Recommendation: NSD-189 must be reformed by the Biden administration to address China's acquisition of critical technology and know-how through fundamental research and Congress must put adequate safeguards on fundamental research.

Problem: BIS argues it is under resourced to carry out its mission.

Recommendation: Amend ECRA to allow BIS to charge fees on certain licenses to better support enforcement efforts.

Problem: BIS has created a loophole that allows China access to potentially sensitive technologies through standard-setting bodies.

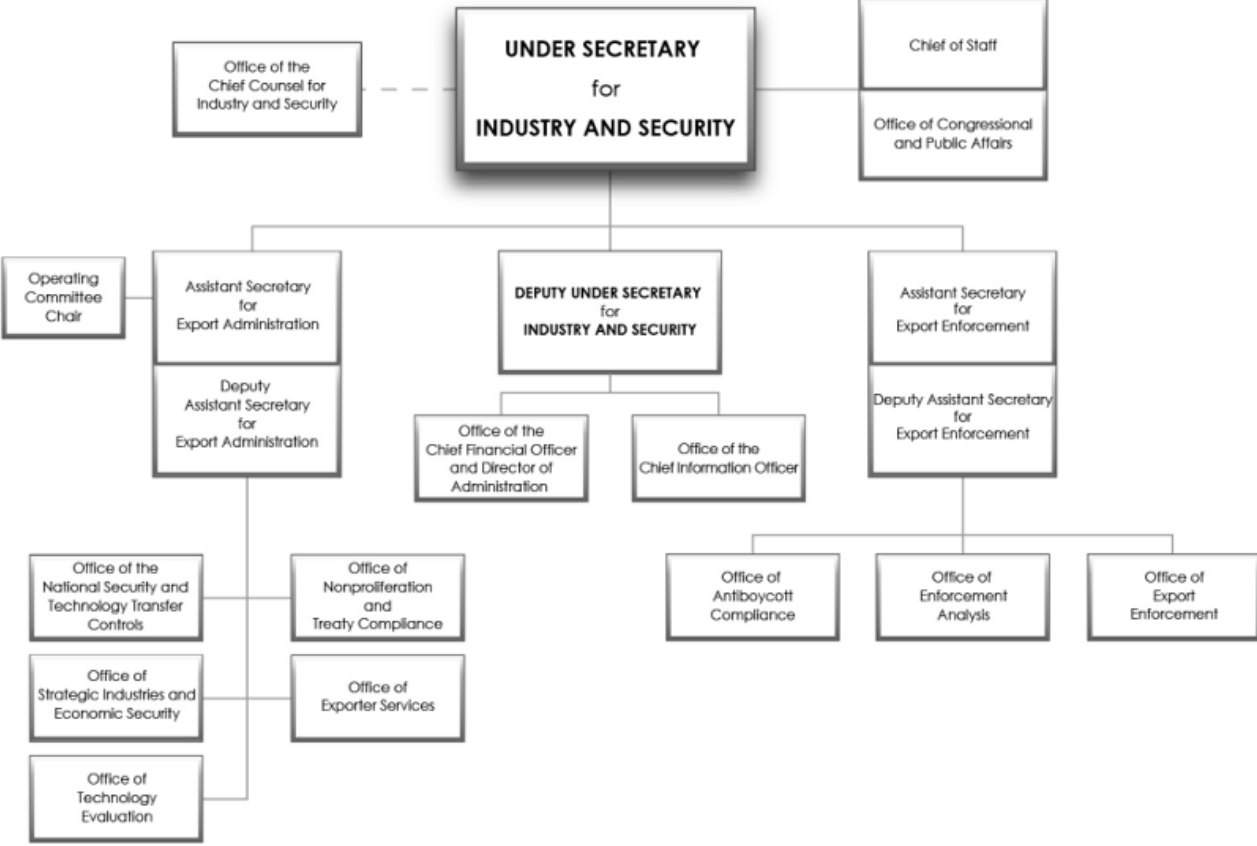
Recommendation: BIS or Congress must update the definition for standard-setting organizations to close this loophole.

APPENDIX II – ORGANIZATIONAL CHART



BUREAU OF INDUSTRY AND SECURITY

U.S. Department of Commerce



APPENDIX III – DEFINITIONS

ABBREVIATION	FULL TERM
CCP	Chinese Communist Party
BIS	The Bureau of Industry and Security
AI	Artificial intelligence
PLA	People’s Liberation Army
MCF	Military-Civil Fusion Strategy
ECRA	<i>Export Control Reform Act of 2018</i>
WMD	Weapons of mass destruction
EAR	Export Administration Regulation
ACEP	Advisory Committee on Export Control Policy
EARB	Export Advisory Review Board
EAR99	Any item not on the Commerce Control List
CCL	Commerce Control List
ERC	End-User Review Committee
APA	Administrative Procedures Review
YMTC	Yangtze Memory Technologies Corp

ABBREVIATION	FULL TERM
MEU	Military End-User
CoCom	Coordinating Committee for Multilateral Export Controls
MOU	Memorandums of understanding
ECO	Export Control Officer
PLC	Pre-license checks
PSV	Post-shipment verifications
PWC	PricewaterhouseCoopers
KPMG	KPMG International Limited
EY	Ernst & Young
NSD	National Security Directive
NSF	National Science Foundation
CFIUS	Committee on Foreign Investment in the United States

-
- [i] "Foreign Companies in China Get a New Partner: The Communist Party," the Wall Street Journal , October 29, 2017, <https://www.wsj.com/articles/foreign-companies-in-china-get-a-new-partner-the-communist-party-1509297523>
- [ii] "National Security Strategy of the United States of America," the White House, December 2017, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- [iii] "Alexander Hamilton's Final Version of the Report on the Subject of Manufactures," December 5, 1791, <https://founders.archives.gov/documents/Hamilton/01-10-02-0001-0007>
- [iv] "Protecting Critical and Emerging U.S. Technologies from Foreign Threats," The National Counterintelligence and Security Center," October 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf
- [v] "ASPI's Critical Technology Tracker – The global race for future power," the Australian Strategic Policy Institute
- [vi] "Rising to the China Challenge," CNAS, January 2020, <https://www.cnas.org/publications/reports/rising-to-the-china-challenge>
- [vii] "Speed Up America, Slow Down China, or Both? The Strategic Question for the 21st Century," ITIF, August 28, 2023, <https://itif.org/publications/2023/08/28/speed-up-america-slow-down-china-key-strategic-question-for-the-21st-century/>
- [viii] "Protecting Critical and Emerging U.S. Technologies from Foreign Threats," The National Counterintelligence and Security Center," October 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf
- [ix] "CIA Future will be defined by US technology race with China, director says," Reuters, March 8, 2023, <https://www.reuters.com/world/us/cia-future-will-be-defined-by-us-technology-race-with-china-director-says-2023-03-08/>
- [x] "Military and Security Developments Involving the People's Republic of China," the Department of Defense, November 2022, <https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>
- [xi] <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- [xii] "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/>
- [xiii] "China's ambitions in artificial intelligence," The European Parliament, September 2021, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA\(2021\)696206_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA(2021)696206_EN.pdf)
- [xiv] "Quotes from Xi: Core technologies must be held in own hands," the People's Daily, May 2023, <http://en.people.cn/n3/2023/0531/c90000-20026119.html>
- [xv] "Comprehensive National Security unleashed: How Xi's approach shapes policies at home and abroad," Mercator Institute for China Studies, September 2022, <https://www.merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and>
- [xvi] "Made in China 2025: Global Ambitions Built on Local Protections," U.S. Chamber of Commerce, 2017, https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf
- [xvii] "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries," Mercator Institute for China Studies, December 2016, https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/MPOC_No.2_Ma deinChina_2025.pdf

[xviii] "Threats to US National Security: Countering PRC's Economic and Technological Plan for Dominance," James Mulvenon, Statement before the Senate Select Committee on Intelligence, March 11, 2022 <https://www.intelligence.senate.gov/sites/default/files/documents/os-jmulvenon-051122.pdf>

[xvix] "Military-Civil Fusion and the People's Republic of China," U.S. Department of State, <https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf>

[xx] "Chinese Technology Transfer Challenges to U.S. Export Control Policy," Dr. Christopher Ashely Ford, July 11, 2018, <https://2017-2021.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/chinese-technology-transfer-challenges-to-u-s-export-control-policy/>

[xxi] "Preventing War in the South China Sea," Journal of Indo-Pacific Affairs, Air University Press, August 2022, <https://www.airuniversity.af.edu/JIPA/Display/Article/3111133/preventing-war-in-the-south-china-sea/>

[xxii] "U.S. Export Controls and China," Congressional Research Service, March 24, 2022, <https://crsreports.congress.gov/product/pdf/IF/IF11627>

[xxiii] "Questions for the Record from Representative Mast: May 11, 2023, <https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf>

[xxiv] "IP Commission Report," February 2017, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf

[xxv] "Special 301 Report," Office of the U.S. Trade Representative, April 2023,

[xxvi] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[xxvii] "Reassessing Threats to US Innovation Posed by China and Implications for Safeguarding Future Supply Chains," Jeffrey Stoff, June 9, 2022, https://www.uscc.gov/sites/default/files/2022-06/Jeff_Stoff_Testimony.pdf

[xxviii] Id.

[xxix] <https://www.congress.gov/bill/117th-congress/house-bill/7776/text?s=3&r=1&q=%7B%22search%22%3A%5B%22hr7776%22%2C%22hr7776%22%5D%7D>

[xxx] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[xxxi] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[xxxii] "How a Big U.S. Chip Maker Gave China the 'Keys to the Kingdom,'" Kate O'Keefe and Brian Spegele, Wall Street Journal, June 27, 2019 <https://www.wsj.com/articles/u-s-tried-to-stop-china-acquiring-world-class-chips-china-got-them-anyway-11561646798>; "China builds advanced weapons systems using American chip technology," Ellen Nakashima and Gerry Shih, The Washington Post, April 9, 2021 https://www.washingtonpost.com/national-security/china-hypersonic-missiles-american-technology/2021/04/07/37a6b9be-96fd-11eb-b28d-bfa7bb5cb2a5_story.html; "American technology boosts China's hypersonic missile program," Cate Cadell and Ellen Nakashima, The Washington Post, October 17, 2022, <https://www.washingtonpost.com/national-security/2022/10/17/china-hypersonic-missiles-american-technology/>

[xxxiii] "China's Top Nuclear-Weapons Lab Used American Computer Chips Decades After Ban," Wall Street Journal, January 29, 2023, <https://www.wsj.com/articles/chinas-top-nuclear-weapons-lab-used-american-computer-chips-decades-after-ban-11674990320>

[xxxiv] "China Uses DNA to Track its People, With the Help of American Expertise," the New York Times, February 21, 2019, <https://www.nytimes.com/2019/02/21/business/china-xinjiang-ughur-dna-thermo-fisher.html>

[xxxv] "China Still Buys American DNA Equipment for Xinjiang Despite Blocks," the New York Times, October 22, 2021, <https://www.nytimes.com/2021/06/11/business/china-dna-xinjiang-american.html>

[xxxvi] "Unfinished Business: Export Control and Foreign Investment Reforms," Emma Rafaelof, U.S.-China Economic and Security Review Commission, June 1, 2021 https://www.uscc.gov/sites/default/files/2021-06/Unfinished_Business-Export_Control_and_Foreign_Investment_Reforms.pdf

[xxxvii] "U.S. Approves Nearly All Tech Exports to China, Data Shows," Wall Street Journal, August 2022, <https://www.wsj.com/articles/u-s-approves-nearly-all-tech-exports-to-china-data-shows-11660596886>

[xxxviii] Nazak Nikhaktar, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[xxxix] 15 CFR § 750.3(b)(1)

[xl] 15 CFR § 740.4(b)(2)

[xli] 15 CFR § 740.4(f)(1)

[xlii] "BIS 2018 Annual Conference on Export Controls and Policy," May 14, 2018, <https://www.bis.doc.gov/documents/bis-annual-conference-2018/2211-mock-operating-committee-breakout-session-rev-13may2018/file>

[xliii] "BIS 2018 Annual Conference on Export Controls and Policy," PowerPoint Presentation, May 14, 2018, <https://www.bis.doc.gov/documents/bis-annual-conference-2018/2211-mock-operating-committee-breakout-session-rev-13may2018/file>

[xliv] 15 CFR § 740.4(f)(2)

[xlv] "BIS 2018 Annual Conference on Export Controls and Policy," PowerPoint Presentation, May 14, 2018, <https://www.bis.doc.gov/documents/bis-annual-conference-2018/2211-mock-operating-committee-breakout-session-rev-13may2018/file>

[xlvi] 15 CFR § 740.4(f)(3)

[xlvii] Id.

[xlviii] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[xlix] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[l] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[li] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[lii] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[liv] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[lv] Id.

[lvi] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[lvii] CFR § 750.3(b)

[lviii] Id.

[lix] Id.

[lx] Id.

[lxi] "Frequently Asked Questions to Export Licensing Requirements," U.S. Department of Commerce Bureau of Industry and Security Office of Exporter Services, <https://www.bis.doc.gov/index.php/documents/pdfs/286-licensing-faq/file#:~:text=EAR99%20items%20generally%20consist%20of,to%20obtain%20an%20export%20license>

[lxii] 15 CFR § 742

[lxiii] "U.S. Export Controls and China," Karen Sutter and Christopher Casey, Congressional Research Service, March 24, 2022. <https://crsreports.congress.gov/product/pdf/IF/IF11627>

[lxiv] Id.

[lxv] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[lxvi] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[lxvii] Id.

[lxviii] Id.

[lxix] Id.

[lxx] Id.

[lxxi] Id.

[lxxii] <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>

[lxxiii] "U.S. Semiconductor Exports to China: Current Policies and Trends," CSET Issue Brief, October 2020, <https://cset.georgetown.edu/publication/u-s-semiconductor-exports-to-china-current-policies-and-trends/>

[lxxiv] "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine," RUSI, August 2022, https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf

[lxxv] BIS U.S. Trade Data with China, <https://www.bis.doc.gov/index.php/country-papers/2575-2019-statistical-analysis-of-u-s-trade-with-china/file>

[lxxvi] <https://foreignaffairs.house.gov/wp-content/uploads/2023/03/BIS-Licensing-Data-Report-Breakdown-PRC-Entities-List16.pdf>

[lxxvii] "U.S. Approves Nearly All Tech Exports to China, Data Shows," Wall Street Journal, August 2022, <https://www.wsj.com/articles/u-s-approves-nearly-all-tech-exports-to-china-data-shows-11660596886>

[lxxviii] <https://www.bis.doc.gov/index.php/documents/pdfs/286-licensing-faq/file>

[lxxix] <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>

[lxxx] 15 CFR § 744.11 License requirements that apply to entities acting or at significant risk of acting contrary to the national security or foreign policy interests of the United States.

[lxxxi] 15 CFR Appendix to Supplement No. 5 to Part 744

[lxxxii] Id.

[lxxxiii] "McCaul Brings Transparency to Tech Transferred to Blacklisted Chinese Companies," Press Release, October 21, 2021 <https://foreignaffairs.house.gov/press-release/mccaul-brings-transparency-to-tech-transferred-to-blacklisted-chinese-companies/>

[lxxxiv] "BIS Approved More than \$23B of Tech Licenses to Blacklisted Companies," Press Release, February 28, 2023, <https://foreignaffairs.house.gov/press-release/bis-approved-more-than-23b-of-tech-licenses-to-blacklisted-companies/>

[lxxxv] https://www.govinfo.gov/content/pkg/USCOURTS-dcd-1_21-cv-01798/pdf/USCOURTS-dcd-1_21-cv-01798-0.pdf

[lxxxvi] Section 1762(a)

[lxxxvii] The 50 percent rule says any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons is itself considered to be a blocked person <https://ofac.treasury.gov/media/6186/download?inline>

[lxxxviii] https://d1tzzns6d79su2.cloudfront.net/uploads/embedded_file/5dfcf76aba02312f44b0564ce030070196d1cb4e1ab90a97fff7b9b6fccea005/72fa44b7-d170-47c8-9052-a678f0632d7d.pdf

[lxxxix] "Scoop: Chinese tech firm sidesteps sanctions," Lachlan Markay, Axios, September 28, 2021, <https://www.axios.com/2021/09/29/chinese-tech-firm-sidesteps-sanctions>

[xc] "Loophole Allows U.S. Tech Exports to Banned Chinese Firms," Ian Talley, Asa Fitch, and Clarence Leong, The Wall Street Journal, March 24, 2023, <https://www.wsj.com/articles/loophole-allows-u-s-tech-exports-to-banned-chinese-firms-b4800164>

[xci] "China's quest for human genetic data spurs fears of a DNA arms race," The Washington Post, September 22, 2023, [Covid helped China secure the DNA of millions, spurring arms race fears - Washington Post](https://www.washingtonpost.com/health/china-quest-for-human-genetic-data-spurs-fears-of-a-dna-arms-race-2023-09-22/)

[xcii] Nazak Nikhaktar Question for the Record, May 11, 2023

[xciii] "Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence," CSET, October 2021, <https://cset.georgetown.edu/publication/harnessed-lightning/>

[xciv] "U.S. Approves Nearly All Tech Exports to China, Data Shows," Wall Street Journal, August 2022, <https://www.wsj.com/articles/u-s-approves-nearly-all-tech-exports-to-china-data-shows-11660596886>

[xcv] <https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>

[xcvi] "U.S. Export Controls and China," Karen Sutter, March 24, 2024, <https://crsreports.congress.gov/product/pdf/IF/IF11627>

[xcvii] "McCaul, China Task Force Members Ask for Honor Device Co. to Be Added to the Entity List," Press Release, August 6, 2021, <https://foreignaffairs.house.gov/press-release/mccaul-china-task-force-members-ask-for-honor-device-co-to-be-added-to-the-entity-list/>

[xcviii] "Rubio, Scott, Cornyn Urge Biden Administration to Add Huawei Spin-off "Honor" to the Entity List," Press Release, October 14, 2021, <https://www.rubio.senate.gov/public/index.cfm/2021/10/rubio-scott-cornyn-urge-biden-administration-to-add-huawei-spin-off-honor-to-entity-list>

[xcix] "China's Recent Trade Measures and Countermeasures: Issues for Congress," Congressional Research Service, December 2021, <https://crsreports.congress.gov/product/pdf/R/R46915>

[c] "Chinese AI groups use cloud services to evade US chip export controls," Financial Times, March 8, 2023, <https://www.ft.com/content/9706c917-6440-4fa9-b588-b18fbc1503b9>

[ci] <https://foreignaffairs.house.gov/wp-content/uploads/2021/07/7.12.21-MTM-Hagerty-letter-to-Sec-Raimondo-re-YMTC50.pdf>

[cii] <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/section-744.21>

[ciii] <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>

[civ] Id.

[cv] "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," New York Times, August 14, 2019, <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>

[cvi] "China tests new space capability with hypersonic missile," The Financial Times, <https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb>

[cvii] "Written evidence submitted by Kevin J. Wolf" U.K. Parliament, <https://committees.parliament.uk/writtenevidence/114084/pdf/>

[cviii] "Trump administration pressed Dutch hard to cancel China chip-equipment sale: sources," Reuters, January 6, 2020, <https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBNIZ50HN>

[cix] "U.S. secures deal with Netherlands, Japan on China chip export limit," Reuters, January 27, 2023 <https://www.reuters.com/world/officials-netherlands-japan-washington-chip-talks-2023-01-27/>

[cx] <https://armscontrolcenter.org/fact-sheet-the-wassenaar-arrangement/>

[cxi] "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force," Press Release, Department of Justice, February 16, 2023 <https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force>

[cxii] §4819. Penalties <https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter58&edition=prelim>

[cxiii] "Western Digital, Seagate Differ on Selling Hard Drives to Huawei," tom'sHARDWARE, September 23, 2020, <https://www.tomshardware.com/news/the-curious-case-of-storage-devices-and-huawei>

[cxiv] "Huawei's Access to Hard Drive Disks in America: An Investigation into Seagate Technology," U.S. Senate Committee on Commerce, Science, & Transportation, October 2021, <https://www.commerce.senate.gov/services/files/2C03C95D-6D36-49FA-8066-52DD1A98A1FE>

[cxv] <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001137789/78f77900-1606-4413-a460-56967befd595.pdf>

[cxvi] "BIS IMPOSES \$300 MILLION PENALTY AGAINST SEAGATE TECHNOLOGY LLC RELATED TO SHIPMENTS TO HUAWEI," Press Release, Bureau of Industry and Security, April 19, 2023 <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3264-2023-04-19-bis-press-release-seagate-settlement/file#:~:text=BIS%20issued%20an%20order%20today,five%2Dyear%20suspended%20Denial%20Order>

[cxvii] "Synopsys Probed on Allegations It Gave Tech to Huawei, SMIC," Bloomberg, April 2023, <https://www.bloomberg.com/news/articles/2022-04-13/synopsys-probed-on-allegations-it-gave-chip-tech-to-huawei-smic#xj4y7vzkg>

[cxviii] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[cxix] Id.

[cxx] Id.

[cxxi] Id.

[cxxii] "Willful Blindness: An Insider's Account of How America's Ineffective Export Control Regime Increases Chinese Military Strength," Stephen Coonen, China Tech Threat, May 10, 2023, <https://chinatechthreat.com/willful-blindness/>

[cxxiii] "China Locks Information on the Country Inside a Black Box," Wall Street Journal, April 30, 2023, <https://www.wsj.com/articles/china-locks-information-on-the-country-inside-a-black-box-9c039928>

[cxxiv] "Chinese authorities raid US due diligence firm Mintz," Financial Times, March 24, 2023, <https://www.ft.com/content/965ca6b4-9d48-4f2d-ad0f-abc6e3a52b15>

[cxxv] "China Closes U.S. Auditor as Tensions Mount Over Forced Labor Allegations," Wall Street Journal, August 19, 2021, <https://www.wsj.com/articles/china-closes-u-s-auditor-as-tensions-mount-over-forced-labor-allegations-11629390253>

[cxxvi] "Big Four Audit Giants Shut Down Legal Operations in China Following 'Regulatory Raids'," Law.com, October 13, 2022, <https://www.law.com/international-edition/2022/10/13/big-four-audit-giants-shut-down-legal-operations-in-china-following-regulatory-raids/?sreturn=20230603134849>

[cxxvii] "China Urges State Firms to Drop Big Four Auditors on Data Risk," Bloomberg, February 22, 2023, <https://www.bloomberg.com/news/articles/2023-02-22/china-urges-state-firms-to-drop-big-four-auditors-on-data-risk?sref=y3YMCJ4e>

[cxxviii] "U.S. Think Tank Reports Prompted Beijing to Put a Lid on Chinese Data," Wall Street Journal, May 2023, <https://www.wsj.com/articles/u-s-think-tank-reports-prompted-beijing-to-put-a-lid-on-chinese-data-5f249d5e>

[cxxix] "Huawei has ran out of chips for smartphones as US sanction crippled the Chinese telecom giant," Techwire Asia, December 2022, <https://techwireasia.com/2022/12/huawei-has-ran-out-of-chips-for-smartphones-as-us-sanction-crippled-the-chinese-telecom-giant/>

[cxxx] "An Interview with Qualcomm CEO Cristiano Amon," Stratechery, May 11, 2023, <https://stratechery.com/2023/an-interview-with-qualcomm-ceo-cristiano-amon/>

[cxxxii] <https://irp.fas.org/offdocs/nsdd/nsdd-189.htm>

[cxxxiii] Id.

[cxxxiv] "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," The IP Commission, 2017, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf

[cxxxv] "China's Quest for Economic, Political Domination Threatens America's Security," February 1, 2022 <https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122>

[cxxxvi] "US Agencies Grappling With Export Control Issues Involving Fundamental Research," Ian Cohen, May 4, 2022, <https://exportcompliance.com/news/2022/05/04/us-agencies-grappling-with-export-control-issues-involving-fundamental-research-2205030045>

[cxxxvii] Nazak Nikakhtar, Questions for the Record, May 11, 2023, Oversight and Accountability Subcommittee

[cxxxviii] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxxxix] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxl] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxli] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxlii] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxliii] Giovanna Cinelli, Questions for the Record, May 11, 2023 Oversight and Accountability Subcommittee

[cxliv] Interview with former BIS official.

[cxlv] <https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security>

[cxlvi] <https://www.congress.gov/bill/117th-congress/senate-bill/3811/text?r=1&s=1>

[cxlvii] U.S. Department of Commerce FY24 Presidential Budget Request for the Bureau of Industry and Security, <https://www.commerce.gov/sites/default/files/2023-03/BIS-FY2024-Congressional-Budget-Submission.pdf>

[cxlviii] 'An Act of War': Inside America's Silicon Blockade Against China, New York Times, July 12, 2023 <https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html>

[cxlix] David Hanke Testimony before the U.S.-China Economic and Security Review Commission, September 8, 2021, https://www.uscc.gov/sites/default/files/2021-08/David_Hanke_Testimony.pdf

[c] "Protecting Critical and Emerging U.S. Technologies from Foreign Threats," the National Counterintelligence and Security Center, October 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf

[cli] "How a Big U.S. Chip Maker Gave China the 'Keys to the Kingdom'," Wall Street Journal, June 27, 2019, <https://www.wsj.com/articles/u-s-tried-to-stop-china-acquiring-world-class-chips-china-got-them-anyway-11561646798>

[clii] "China Exploits Fleet of U.S. Satellites to Strengthen Police and Military Power," Wall Street Journal, April 2019, <https://www.wsj.com/articles/china-exploits-fleet-of-u-s-satellites-to-strengthen-police-and-military-power-11556031771>

[cliii] "AI companies are enabling genocide in China," The Washington Post, April 12, 2021, <https://www.washingtonpost.com/opinions/2021/04/12/china-is-using-ai-repress-uyghurs-it-must-stop/>

[cliv] "Unfinished Business: Export Control and Foreign Investment Reforms," Emma Rafaelof, U.S.-China Economic and Security Review Commission, June 1, 2021 https://www.uscc.gov/sites/default/files/2021-06/Unfinished_Business-Export_Control_and_Foreign_Investment_Reforms.pdf

[clv] <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf>

[clvi] <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>

[clvii] "Made in China 2025: Global Ambitions Built on Local Protections," U.S. Chamber of Commerce, https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf

- [clviii] "U.S. Secretary of Commerce Penny Pritzker Delivers Major Policy Address on Semiconductors at Center for Strategic and International Studies," November 2016, <https://2014-2017.commerce.gov/news/secretary-speeches/2016/11/us-secretary-commerce-penny-pritzker-delivers-major-policy-address.html>
- [clix] "Wassenaar Arrangement 2014 Plenary Agreements Implementation and Country Policy Amendments," <https://www.federalregister.gov/documents/2015/05/21/2015-10579/wassenaar-arrangement-2014-plenary-agreements-implementation-and-country-policy-amendments>
- [clx] "Foreign Availability Determination: Anisotropic Plasma Dry Etching Equipment," <https://www.federalregister.gov/documents/2015/02/09/2015-02681/foreign-availability-determination-anisotropic-plasma-dry-etching-equipment>
- [clxi] "Semiconductors and the CHIPS Act: The Global Context," CRS, September 28, 2023, https://www.everycrsreport.com/files/2023-09-28_R47558_321f52a4e7b8f2c4225f36c7c0316cfa3aeef9ac.pdf
- [clxii] "China's Got a New Plan to Overtake the U.S. in Tech," Bloomberg, May 20, 2020, <https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech#xj4y7vzkg>
- [clxiii] <https://www.federalregister.gov/documents/2022/09/09/2022-19415/authorization-of-certain-items-to-entities-on-the-entity-list-in-the-context-of-specific-standards>
- [clxiv] "Submission of the U.S. Chamber of Commerce for the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation" October 3, 2017, <https://www.regulations.gov/comment/USTR-2017-0016-0054>
- [clxv] "Made in China 2025: Global Ambitions Built on Local Protections," U.S. Chamber of Commerce, https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf



**FOREIGN AFFAIRS
COMMITTEE**

CHAIRMAN MCCAUL

