

THE DECISIVE DECADE:

Advancing National Security at the Department of Commerce



“[O]ur world is at an inflection point. How we respond to the tremendous challenges and the unprecedented opportunities we face today will determine the direction of our world and impact the security and prosperity of the American people for generations to come ... [We must] seize this decisive decade to advance America’s vital interests, position the United States to outmaneuver our geopolitical competitors, tackle shared challenges, and set our world firmly on a path toward a brighter and more hopeful tomorrow.”

– President Joseph R. Biden

December 2024

FOREWORD

A Special Message From:

Deputy Secretary Graves, U.S. Department of Commerce



The Department of Commerce has never been so central to U.S. national security as it is today. *The Decisive Decade: Advancing National Security at the Department of Commerce* was developed in response to unprecedented threats and disruptions to the country's national and economic security in areas over which the department has powerful analytical tools and unique capabilities. That is why I am proud to release this first-ever Commerce strategy on national security. Recognizing that economic security is critical to our national security, this strategy was created to guide implementation of the Biden-Harris Administration's National Security Strategy at the Department of Commerce. It provides a framework to guide the Department in bolstering national resilience to disruptions, defending against immediate threats, and creating conditions that ensure other threats never materialize in the first place.

Congress and the Biden Administration have entrusted our Department with critical national security authorities, including an expanded export control regime, and crucial funding to invest in critical and emerging technologies in communities across the country through the CHIPS and Science Act.

Given these new tools and responsibilities, we have — and must continue to — reevaluate our agency's vital role in our country's national security landscape.

Since the release of the Administration's strategy, I have been privileged to lead several Department-wide efforts to guide its implementation. These include an inter-bureau Critical Emerging Technology Threats (CETT) group which routinely receives intelligence briefings and works to develop a coordinated approach to confront challenges posed by promising new and advancing technologies such as AI, biotechnologies, clean energy technology, and quantum information sciences. I also spearheaded the realignment of our Office of Intelligence to better address Department-wide intelligence support and coordination. This realignment, which was recently approved by our partners in Congress, will help us realize the goals outlined in this strategy.

Both examples underscore two key principles driving our work. First, the execution of our national security responsibilities must be a whole-of-Department effort — every bureau plays a role in this critical mission. Second, our Department must be proactive in addressing national security threats. Imminent threats demand immediate responses, but some of our most important work is — and will continue to be — preventing threats from arising in the first place.

The strategy is organized into five pillars which highlight our bureaus' tools, authorities, and efforts in the national security space for our partners in government, abroad, and in the private sector: (1) Critical and Emerging Technologies (CET), (2) Global Peace, Stability, and Security, (3) Cybersecurity and the Digital Economy, (4) Critical Supply Chains, and (5) Safe Environments.

Each pillar includes a call for public and private investment and partnership to advance U.S. national security and competitiveness. Our primary goals and priorities include:

- Strengthening U.S. CET leadership through focused investment and partnership;
- Ensuring global security by building capacity and international partnerships;
- Expanding private sector coordination for cybersecurity and the digital economy;
- Deepening analytic capacity and partner engagement to build and protect critical supply chains; and
- Leveraging the Department's data and research to enable safe environments.

The collaboration required to create this strategy is a significant step in an ongoing process to evaluate and respond to a rapidly evolving threat landscape confronting our nation, but there is more to be done. Achieving the goals outlined above will require targeted investment to support scaling critical and emerging technologies and additional resources to bolster the Department's ability to counter growing threats from our adversaries. We must also continue to seek cooperation with our allies and partners and work closely with industry to promote the widespread adoption of science-based standards.

The Secretary and I are grateful for the support we received from our colleagues within the Department of Commerce, the Intelligence Community, the National Security Council, and across the U.S. Government in developing this strategy.

Sincerely,



Don Graves
Deputy Secretary
U.S. Department of Commerce

TABLE OF CONTENTS

TABLE OF CONTENTS	4
INTRODUCTION	5
SPECTRUM OF DOC NATIONAL SECURITY TOOLS	9
PILLAR 1:	10
CRITICAL AND EMERGING TECHNOLOGIES	10
The Challenge	10
Strategic Objectives	11
PILLAR 2:	18
GLOBAL PEACE, STABILITY, AND SECURITY	18
The Challenge	18
Strategic Objectives	19
PILLAR 3:	23
CYBERSECURITY AND THE DIGITAL ECONOMY	23
The Challenge	23
Strategic Objectives	24
PILLAR 4:	28
CRITICAL SUPPLY CHAINS	28
The Challenge	28
Strategic Objectives	29
PILLAR 5:	33
SAFE ENVIRONMENTS	33
The Challenge	33
Strategic Objectives	34
GOING FORWARD	37

INTRODUCTION

President Biden has declared that the world is at an inflection point. How the United States responds to the scale and scope of today's national security challenges will determine not only American security and prosperity, but global security and prosperity as well – for generations to come.

The Commerce Department has never been so central to ensuring U.S. national security as it is today. In the Biden-Harris Administration, Commerce Department leadership engagement with the National Security Council increased significantly as compared to the previous fifteen years. Our long-standing work to advance our core mission to foster economic growth has taken on increased importance for national security in recent years.

Acute shocks and long-term trends have led us to this critical moment. The COVID-19 pandemic laid bare vulnerabilities in our supply chains following the decades-long hollowing out of our industrial base. Russia's unprovoked illegal war in Ukraine became the largest land war in Europe since World War II, bringing together a global coalition of countries to cut off Russia's access to resources to fuel its war.

Our strategic environment has also transformed in the last decade. We now live in an era of strategic competition and interdependence.¹ The People's Republic of China (PRC) is the only state with both the intent and power to reshape the international order that has governed for the last three-quarters of a century, a problem exacerbated by the breakneck pace of technological development, global democratic backsliding, and greater challenges to global governance. Meanwhile, the PRC and the United States are economically interdependent and share interests in addressing transnational problems, such as the systemic threat of climate change.²

The complexity of the China challenge is rooted in the increasingly interconnected relationship between economics, science, technology, and national security. The Department of Commerce sits at that very nexus.

To meet these growing challenges, the Department has also assumed new responsibilities. Front and center are efforts to advance the domestic industrial base, starting with our work to rebuild the critical semiconductor supply chain. In tandem, the Department has adopted a new approach to domestic economic development. We have made transformative investments in

¹ Sullivan, Jake. *The Sources of American Power*. Foreign Affairs, October 24, 2023. <https://www.foreignaffairs.com/united-states/sources-american-power-biden-jake-sullivan>.

² Sullivan, Jake. *Remarks and Q&A by National Security Advisor Jake Sullivan on the Future of U.S.-China Relations*. The White House, January 30, 2024. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2024/01/30/remarks-and-qa-by-national-security-advisor-jake-sullivan-on-the-future-of-u-s-china-relations/>.

innovation and community outreach, through the CHIPS and Science Act,³ Regional Technology and Innovation Hub (Tech Hub) Program, Build Back Better Regional Challenge (BBBRC), and Broadband Equity Access and Deployment Program (BEAD), among others, to ensure that technologies critical to national security are invented, commercialized, and manufactured in the United States.

The Department has stepped up its work to promote international supply chain resilience, too. Building on its long-standing role in commercial diplomacy, the Department has advanced innovative supply chain agreements, launched a first-of-its-kind Supply Chain Center, and promoted friendshoring. To respond to a changing technology environment, the Department recently stood up a new office to address information and communication technology and services (ICTS) threats, reorganized and elevated the Office of Space Commerce, has driven wireless innovation through the Innovation Fund, and is becoming the center of the U.S. Government's efforts on AI innovation and safety work through work at the National Institute of Standards and Technology (NIST) including efforts at the new AI Safety Institute.

As we have promoted technological leadership at home, we have also taken steps to protect our most advanced technologies from being weaponized against us. We have issued export controls with greater significance and frequency than ever before and established new collaborative enforcement mechanisms within the U.S. Government as well as with partners and allies. We have helped to establish a new outbound investment regime to ensure that U.S. dollars do not help our adversaries develop new capabilities that undermine our national security. The Department also continues to lead in R&D for several critical and emerging technologies such as quantum technologies, biotechnology, and AI, while it protects a burgeoning repository of critical national data. This work helps to ensure our economic resilience against diverse foreign threats.

But there is more to be done. The Department must continue to adapt to this expanded national security role. To guide this continuing transition, *The Decisive Decade: Advancing National Security at the Department of Commerce* stitches together the many equities, programs, and authorities that are relevant to national security across the Department. Drawing from the Biden-Harris Administration's 2022 National Security Strategy⁴ and the Department's

³ Raimondo, Gina M. *Remarks by U.S. Secretary of Commerce Gina Raimondo: The CHIPS Act and a Long-term Vision for America's Technological Leadership*. U.S. Department of Commerce, February 23, 2023. <https://www.commerce.gov/news/speeches/2023/02/remarks-us-secretary-commerce-gina-raimondo-chips-act-and-long-term-vision>.

⁴ The White House. *National Security Strategy*, 33. October 12, 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>.

2022-2026 Strategic Plan,⁵ this strategy captures the Department's many national security roles and aligns them under a single, forward-looking, and holistic framework that matches programs with goals to help steward the Department's resources most effectively.

This strategy serves several purposes of institutional adaptation for Department staff and leadership, but its importance is not limited to the efficiency and success of the Department's own work. Transparency, coherence, and clarity on national security issues benefit both internal and external stakeholders. For other agencies in the U.S. Government, the strategy highlights where and how the Department can support national security goals across the executive branch. For partners and allies, it assures a firm commitment to shared values and priorities, with a blueprint for furthering them. For the private sector, greater clarity translates to greater predictability for business operations and continued prosperity. Even for adversaries, transparency and communication can help avoid misperception and miscalculation that can lead to dangerous escalation.

In the national security context, the Department's goals are *strategic resilience, defense, and threat prevention*: to affirmatively bolster the country's resilience to national security threats, to defend the United States and its values against direct or immediate threats, and to help create conditions that ensure other threats never appear on the horizon at all. Our approach is guided by three overarching principles. First, we must employ a *whole-of-department approach*. The Department's national security work spans everything from the floor of the ocean to the surface of the sun. Every bureau plays a role and complements one another. And the same is true of other departments and agencies, especially those with deep national security experience and expertise. Second, the Department must be *proactive, not just reactive*. Immediate threats will demand responses in the moment, but the more the Department can prevent, mitigate, delay, or impede future threats, the more secure the country will be. Third, our strategy emphasizes the *importance of partners and the private sector*. No other government agency parallels the breadth and depth of our industry relationships or expertise in commercial diplomacy. When the Department responds to a threat, it values tailored approaches — with deep multilateral and industry engagement — to amplify impact and avoid unintended consequences.

These principles inform the Department's use of its unique authorities and capabilities to address five pillars of effort: (1) Critical and Emerging Technologies (CET), (2) Global Peace, Stability, and Security, (3) Cybersecurity and the Digital Economy, (4) Critical Supply Chains, and (5) Safe Environments. These pillars are not mutually exclusive; the missions, tools, and activities of bureaus are intended to overlap across the pillars.

⁵ U.S. Department of Commerce. *Strategic Plan: Innovation, Equity, and Resilience: Strengthening American Competitiveness in the 21st Century*, 42. March 2022. <https://www.commerce.gov/sites/default/files/2022-03/DOC-Strategic-Plan-2022%E2%80%932026.pdf>.

At the very heart of this strategy is the human dimension of national security. The Department directly impacts the welfare and prosperity of millions of Americans. To that end, every goal aims to protect the American people against threats and disruptions, now and in the future, and to promote equitable and inclusive economic and digital policies that advance the common good.

The national security challenges our nation faces are significant, complex, and necessitate the urgent and full use of the Department's resources, alongside coordination with other agencies, the private sector, and our partners and allies. As this strategy explains, the Department and its greatest asset – dedicated public servants who work tirelessly for the benefit of the country – are up to the task. Together, we can, and will, ensure America remains free, secure, and prosperous.

SPECTRUM OF DOC NATIONAL SECURITY TOOLS

The Department has a range of tools to support national security efforts. Below is a non-exhaustive list that captures many of these tools. The pillars of effort in the following sections discuss the optimal balance of these resources to achieve topical national security priorities.

	Tools to Support National Security	BIS	EDA	ITA	MBDA	NIST	NOAA	NTIA	OUSEA	USPTO	CLDP
Soft Power Tools	Data Collection/Publishing	♦	♦	♦	♦		♦	♦	♦	♦	
	Metrology					♦					
	Federal Lab R&D					♦	♦	♦			
	Public-Private Research Partnerships					♦	♦	♦			
	Standards Development	♦		♦		♦	♦	♦	♦	♦	♦
	Issuing Reports, Guidance, and Best Practices	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
	Weather/Space Weather Prediction/Climate Modeling						♦				
	Industry Analysis	♦		♦		♦	♦	♦	♦	♦	
	Industry Convening/Engagement	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
	Int'l Fora/Institutional Participation	♦		♦		♦	♦	♦	♦	♦	♦
Hard Power Tools	Commercial Diplomacy/Personnel Abroad	♦		♦			♦			♦	♦
	Trade Promotion (Exports, Inbound FDI)			♦				♦			♦
	Fast-Track Patent Processes									♦	
	Grant Making/Awards Programs		♦	♦	♦	♦	♦	♦		♦	
	Technical and Legal Assistance/Capacity Building Abroad	♦		♦			♦	♦		♦	♦
	Interagency Personnel Exchanges	♦		♦		♦	♦	♦		♦	♦
	Environmental Monitoring/Mapping						♦				
	Space Situational Awareness Monitoring						♦				
	Treaty Compliance/Trade Monitoring	♦		♦			♦			♦	♦
	Emergency Response and Recovery	♦	♦				♦	♦			
	Inbound Investment Review	♦		♦				♦			
	Outbound Investment Restrictions	♦		♦							
	Defense Priorities and Allocations Systems (DPAS) Actions	♦									
	Tariffs (Duties/Investigations)	♦		♦							
	Trade Restrictions/Licensing Regimes	♦		♦			♦	♦	♦		
	Rulemaking/Regulation	♦	♦	♦		♦	♦	♦	♦	♦	
	Limited Operations on Commercial Remote Sensing Space Systems						♦				
	Law Enforcement	♦					♦				

Note: NIST's research and development authorities do not involve rulemaking.

PILLAR 1: CRITICAL AND EMERGING TECHNOLOGIES

GOAL	Protect and Strengthen U.S. Innovation and Leadership in Critical and Emerging Technologies (CET)
STRATEGIC OBJECTIVES	1.1 Drive CET innovation through R&D 1.2 Scale up and support CET industries 1.3 Facilitate innovative and trusted CET ecosystems 1.4 Prevent adversaries from accessing, developing, and exploiting CET to harm U.S. national security

The Challenge

Today's pace of technological innovation is staggering. As President Biden has remarked, the world will witness more technological change in the next few years than in the last fifty.⁶ Critical and emerging technologies (CET) — including quantum information science, semiconductors and microelectronics, artificial intelligence (AI), biotechnology and biomanufacturing, clean energy, next-generation communications, advanced computing, data security, and space technologies — are driving this transformation.⁷ These technologies will increasingly underpin how societies function, interact, and grow.⁸

This foundational quality captures the core challenge of the rapid and high stakes technological competition between democratic and autocratic societies. Leadership in CET development matters significantly, since the norms and regulations around their use, deployment, and governance are not foreordained. This means that CET leadership does not only confer specific economic and military advantages in the moment. Those advantages become self-reinforcing over time, precisely because CET are so foundational. Given this flywheel effect, any ground the United States and likeminded nations lose on certain foundational technologies in the immediate future not only threatens Americans today, it weakens the future promise of a democratic world and fair economic system.

⁶ Biden, Joseph. *Remarks by President Biden on Artificial Intelligence*. The White House, July 21, 2023. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/07/21/remarks-by-president-biden-on-artificial-intelligence/>.

⁷ White House Office of Science and Technology Policy. *White House Office of Science and Technology Policy Releases Updated Critical and Emerging Technologies List*. February 12, 2024. <https://www.whitehouse.gov/ostp/news-updates/2024/02/12/white-house-office-of-science-and-technology-policy-releases-updated-critical-and-emerging-technologies-list/>.

⁸ Sullivan, Jake. *Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit*. The White House, 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/>.

The United States and its allies have traditionally led in the development and production of CET. But this leadership is threatened by intense global competition, especially with the PRC. Critical technologies that were invented in the United States, like solar panels, moved overseas during the scale up process due to limited U.S. production capacity. U.S. leadership in advanced manufacturing, which relies on learning by doing, has been threatened. For instance, the United States used to be a leader in global semiconductor manufacturing, but today manufactures only 10% of the world's chips — and 0% of the most advanced chips.

Building and maintaining CET leadership will allow the United States to best channel these technologies for societal good, to reflect democratic norms and privacy rights, and to enable companies to compete fairly on a level playing field necessary for innovation and prosperity, all while ensuring security and safety. An alternative, authoritarian model embraces abuse of CET innovation, normalizes rampant intellectual and data theft that undermines innovation, and grants leverage over the world's critical infrastructure. The less this authoritarian model proliferates, the greater freedom and prosperity will be assured in the United States and globally.

Strategic Objectives

- 1.1 Drive CET innovation through R&D:** Invest in research to discover CET innovations in the lab.
- 1.2 Scale up and support CET industries:** Assist the private sector in manufacturing, protecting IP, and commercializing to deploy innovation at scale.
- 1.3 Facilitate innovative and trusted CET ecosystems:** Influence the larger operating environment for innovation through government-led policy.
- 1.4 Prevent adversaries from accessing, developing, and exploiting CET to harm U.S. national security:** Blunt, delay, and raise costs of adversarial advancement in CET that could harm U.S. and allied national security interests.

1.1 Drive CET innovation through R&D

CET innovation begins in the lab. The Department plays a direct role in developing CET innovations through R&D at federal laboratories at NIST, NOAA, and NTIA. Their many research streams help to directly advance CET research including, for example, at NTIA's Institute for Telecommunications Sciences and NIST's novel fundamental measurement science results and methods published in technical reports and top-tier scientific journals. The Department also collaborates on R&D with other federal agencies, such as the National Science Foundation and the Department of Energy.

To support R&D, the Department has numerous cooperative agreements, including federally funded research and development centers (FFRDCs), joint institutes, cooperative institutes, and public-private research partnerships such as NIST's new partnership with the National Science Foundation's Institute for Trustworthy AI in Law & Society (TRAILS), the World Intellectual Property Organization (WIPO) Green partnership, and National Oceanic and Atmospheric Administration's (NOAA's) Industry Proving Ground and cooperative work on modeling, sensors, and uncrewed systems. The United States Patent and Trademark Office (USPTO)'s intellectual property (IP) expertise is also critical for ensuring that IP is adequately protected and enforced, especially against foreign threats. These partnerships mutually expand capabilities, leveraging the convening power of the Department to enable greater scientific collaboration. And USPTO incentivizes innovation by creating fast-track patent processes for priority sectors. By investing directly in R&D at home, the Department helps ensure that the United States leads in CET innovation from the very start.

These activities directly advance CET innovation and U.S. leadership, but they also carry their own risks. For that reason, research should be guided by the Office of Science and Technology Policy's (OSTP's) National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development implementation guidance.⁹

1.2 Scale up and support CET industries

CET must be consistently available at scale, but the market alone cannot guarantee that outcome. The last half century has revealed the failures of a hands-off approach to CET industries. The semiconductor industry is but one example where the United States lost its position of leadership in the face of foreign subsidies and market responses to those distortions, opening the door for competitors and adversaries to aggressively establish their own tech advantage, thereby undermining U.S. national security.¹⁰ Market failures are also to blame. At the early stages of technology development, the risks may be so great and the rewards so difficult to capture that private actors have difficulty making the critical investments necessary to commercialize CET industries. The United States must build more. That belief is at the heart

⁹ National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. The White House, January 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>.

¹⁰ Graves, Don. *Remarks by Deputy Secretary of Commerce Don Graves at Information Technology Industry Council*. U.S. Department of Commerce, January 31, 2023. <https://www.commerce.gov/news/speeches/2023/01/remarks-deputy-secretary-commerce-don-graves-information-technology-industry>.

of this Administration's modern industrial and innovation strategy,¹¹ and the Department helps invest in the country's economic and technological strength in many ways beyond direct R&D support.

The Department has advanced policy solutions to help the many companies that need help traversing the "valley of death" between basic research and commercialization. These include Department initiatives that promote public-private partnership in innovation, like NIST's Quantum Economic Development Consortium and Manufacturing USA institutes and NOAA's Technology Partnerships Office. In recent years, the Department has established new models and authorities. The Economic Development Administration's (EDA's) Tech Hubs program designated 31 Tech Hubs across the country and invested \$504 million in implementation grants to 12 Tech Hubs to scale up the production of critical technologies and strengthen U.S. economic competitiveness.¹² Technologies targeted for scale up range from quantum and biomanufacturing to semiconductors and clean energy. The National Telecommunications and Information Administration (NTIA) administered Public Wireless Supply Chain Innovation Fund provides direct financial assistance to firms to tackle outstanding barriers to integration and deployment of Open Radio Access Networks (ORAN). In addition, the NIST-administered CHIPS R&D Notices of Funding Opportunity (NOFOs) aim to establish the capacity to invent, develop, prototype, and deploy the foundational semiconductor technologies of the future here in America. The National Semiconductor Technology Center (NSTC) funded by the CHIPS and Science Act, is a public-private consortium that will convene industry, academia, and government from across the semiconductor ecosystem to address the most challenging barriers to continued technological progress in the domestic semiconductor industry, including the need for a skilled workforce. A key goal is to significantly reduce the time and cost of moving from design ideation to commercialization.¹³

With certain critical industries, as with semiconductors, our national security demands a robust and world-leading domestic manufacturing base.¹⁴ With the passage of the CHIPS and Science Act, the Department has a new role in directly incentivizing and sustaining robust CET production. The CHIPS Program Office, established at NIST, has attracted extraordinary

¹¹ For "modern industrial and innovation strategy," see Sullivan, Jake. *Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution*. The White House, April 27, 2023. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/>.

¹² U.S. Economic Development Administration. *Tech Hubs Aim to Make United States the Global Leader in Technologies of the Future: A Conversation with Eric Smith*. October 20, 2023. <https://www.eda.gov/news/blog/2023/10/20/tech-hubs-aim-make-united-states-global-leader-technologies-future>.

¹³ National Institute for Standards and Technology. *A Vision and Strategy for the National Semiconductor Technology Center CHIPS Research and Development Office*. April 27, 2023. <https://www.nist.gov/system/files/documents/2023/04/27/A%20Vision%20and%20Strategy%20for%20the%20NSTC.pdf>.

¹⁴ National Institute for Standards and Technology. *Vision for Success: Commercial Fabrication Facilities*. February 13, 2023. <https://www.nist.gov/chips/vision-success-commercial-fabrication-facilities>.

technical, investment, legal and policy talent to develop strategy, conduct due diligence, and assess risk, as required when granting funds to private firms at later stages in technology development.

U.S. CET leadership also relies in part on the ability of U.S. companies to sell their products abroad. This capability relies on workforce development, trade and export promotion, industry analysis, industry convenings, IP guidance, and initiatives such as the CHIPS NSTC, EDA's Tech Hubs and BBBRC programs, and attracting foreign direct investment such as by aggressively encouraging trusted foreign firms in CET to establish production facilities and R&D centers in the United States. The Department's trade and export promotion services support this work.

With CET, however, the United States should not and cannot go it alone.¹⁵ Our goal has never been for the United States to be completely self-sufficient with respect to CET. The goal is to prevent over-reliance on one country or region, particularly an adversary. Investment at home enables the United States to be a better partner internationally. The Department is committed to working with friends and allies, not just to help build trusted and resilient global supply chains, but also to support CET industries of friends and allies through, for instance, technical assistance, information sharing, and analysis.

1.3 Facilitate innovative and trusted CET ecosystems

To enable CET innovation, the Department also influences the larger innovation ecosystem. This means government policy to create an innovation-friendly business environment, such as through standards and policy development both domestically and internationally, open data sharing, broader investment at home and abroad, efforts to open new markets, and fast-tracking patent processes. Not only does this vital work contribute to a thriving economy and U.S. CET leadership, it helps ensure technology ecosystems now and in the future are open, trusted, interoperable, reliable, and secure.¹⁶ These shared values promote better and more predictable business environments for the private sector to flourish and foster norms of responsible development and use and stronger IP protection, important for all CET. Ensuring safe, secure, and trustworthy technology development is especially urgent for generative artificial intelligence (AI). That is why the Department launched the AI Safety Institute (USAISI), building on NIST's trustworthy AI research, to develop the tools needed to measure models' capabilities and risks, promote safe and secure AI adoption, and facilitate a private

¹⁵ See Graves, Don. *Remarks by Deputy Secretary of Commerce Don Graves at Temple University Japan*. U.S. Department of Commerce, September 14, 2023. <https://www.commerce.gov/news/speeches/2023/09/remarks-deputy-secretary-commerce-don-graves-temple-university-japan>.

¹⁶ White House, *National Security Strategy*, 33.

sector ecosystem of trusted evaluators.¹⁷ USAISI will work with the AI sector to build a solid technical foundation for securing U.S. AI systems, maintain U.S. AI leadership, and prevent adversaries from misusing American innovations to undermine American national security.

This work cannot be successful without deep international engagement. As noted above, it is neither realistic nor desirable to produce every component of every critical technology in this country. Instead, our goal is to enable trusted ecosystems that *include* our allies abroad (e.g., by friendshoring) to ensure our adversaries cannot gain an advantage in CET that they can leverage against us.¹⁸ The Department's efforts to build an international network of AI safety institutes, achieve consensus on the G7 AI Principles and Code of Conduct, and develop international policy on IP rights and export controls illustrate the urgent priority to work in concert with partners and allies.

1.4 Prevent adversaries from accessing, developing, and exploiting CET to harm U.S. national security

Innovating, commercializing products, and shaping trusted ecosystems together help the United States “run faster” in CETs. But it is equally important in the CET innovation race to “slow down” adversaries who would use our own CET innovations to harm our national security interests, including through efforts to modernize their militaries. It is common sense to prevent transfers of sensitive technology to an adversary that threatens to use our innovations against us or our allies.¹⁹

The Department has many tools to deny such transfers. To begin, we can block adversary access to sensitive U.S. technology and know-how through regulatory means. The Bureau of Industry and Security's (BIS) export controls are some of the Department's most important tools for protecting CET.

For decades, BIS has focused on slowing the proliferation of nuclear, chemical, and biological weapons and impairing the military advancement of and human rights abuses by adversaries, including non-state actors that might employ dual-use technologies for terrorism or to destabilize countries and regions. But in the last two decades, rapid technological developments

¹⁷ National Institute for Standards and Technology. *The United States Artificial Intelligence Safety Institute: Vision, Mission, and Strategic Goals*. May 21, 2024. <https://www.nist.gov/system/files/documents/2024/05/21/AISI-vision-21May2024.pdf>.

¹⁸ For more on friendshoring and related strategies, see section 4.3 below.

¹⁹ See Sullivan, Jake. *Remarks and Q&A by National Security Advisor Jake Sullivan at the 2024 World Economic Forum / Davos, Switzerland*. The White House, January 16, 2024. <https://www.whitehouse.gov/briefing-room/speeches-remarks/2024/01/16/remarks-and-qa-by-national-security-advisor-jake-sullivan-at-the-2024-world-economic-forum-davos-switzerland/>.

and the emergence of the PRC as a strategic competitor poses new national security challenges.²⁰ For example, in the rapidly developing field of AI, BIS is accelerating efforts to develop appropriate and effective controls to safeguard U.S. national security and foreign policy interests in the AI space. BIS also oversees vastly more commerce than even a decade ago. Since 2010, total U.S. exports are up 58 percent, and exports under BIS licenses are up 176 percent.

Against this backdrop of rapid innovation, increased adversary threats, and expanding trade volumes, BIS faces a formidable challenge in advancing U.S. national security and foreign policy interests through export controls. BIS Export Administration (EA) has leveraged its regulatory authority in innovative ways to meet this challenge. The pace of publication for BIS regulations has increased to address rapidly evolving performance parameters in advanced technology, such as semiconductors. And BIS has increased its use of foreign direct product rules (FDPRs) since 2020 to cover CET produced abroad with certain U.S. software, technology, or production equipment to address national security concerns amid increasingly complex global supply chains. In addition to list-based controls on CET whose performance parameters make them inherently capable of supporting adversaries' destabilizing military activities, BIS has also increased export restrictions on specific activities, such as advanced semiconductor manufacturing and supercomputing in adversary nations, and entities of concern. For example, over 70 percent of the entities listed on BIS's Entity List, which restricts trade with entities acting contrary to U.S. national security and foreign policy interests, were added during the Biden-Harris Administration.

The Department has also strengthened enforcement of export controls. BIS Export Enforcement (EE) is bringing more cases than ever. BIS has also sought new interagency coordination mechanisms such as the Disruptive Technology Strike Force (DTSF). Co-led with the U.S. Department of Justice, the DTSF aims to counter the threat posed by the acquisition of sensitive, advanced technologies by nation-state adversaries like the PRC. USPTO helps to protect against CET national security threats through pre-publication review of patent applications in certain circumstances. Other major regulatory tools include inbound investment review and outbound investment restrictions, IP protection, and technology guardrails. The Department also shares information to guide industry, academia, partners, and allies away from engaging with adversaries on CET and to promote trusted CET alternatives, at home and abroad.

While protecting national security is paramount, different methods to reach that goal will have different risks, tradeoffs, and limitations. In choosing between potential actions, our objective is to act decisively to constrain adversarial capabilities while taking care not to unduly compromise

²⁰ Bureau of Industry and Security. *Under Secretary of Commerce for Industry and Security Alan F. Estevez Keynote Remarks*. March 28, 2024. <https://www.bis.gov/speeches/under-secretary-commerce-industry-and-security-alan-f-estevez-keynote-remarks>.

the international competitiveness of U.S. industry or create substantial economic uncertainty.²¹ When adversaries have alternatives, some unilateral actions risk inflicting economic costs on U.S. industry without any appreciable national security benefit. So even as we pursue policies to ensure that our adversaries do not gain access to cutting-edge CET, links to less advanced U.S. technologies could in some cases undercut adversary attempts to indigenize.

Adversaries will also continue to look for creative ways to sidestep and undermine our controls, including by finding substitutes, or strengthening their indigenous capabilities. Thus, the Department must regularly and rigorously monitor, update, and adapt our controls in response, especially in periods when our adversaries are fully committed to indigenization but still rely on U.S. technology. CET innovation is a moving target, and we should expect adversaries to constantly pursue ways to circumvent our efforts and aggressively investigate and penalize violators. Delaying adversary military modernization and increasing its cost will often be the realistic measures of success.

The Department's strategic approach is narrowly tailored to avoid overreach that could stifle innovation or impede legitimate commercial activity. Before acting, the Department, in coordination with other departments and agencies, strives to analyze the effectiveness of planned actions and the likely impacts to the national security of the United States, which includes U.S. technology leadership, as well as likely impacts to allies and partner countries. We also seek to work with allies and partners to ensure that our controls are effective, and that allied firms cannot undercut U.S. competitors in adversary countries. Though some circumstances may be so significant as to demand unilateral action, multilateral alignment increases the effectiveness of U.S. actions. In sum, the Department's approach challenges old-fashioned thinking that enabling innovation and protecting national security are direct, one-to-one tradeoffs over the long term. They are not. We can do both, and we must do both.²²

²¹ See Bureau of Industry and Security. *Guiding Principles for the Export Control System*. U.S. Department of Commerce. Accessed 2024. <https://www.bis.gov/guiding-principles>.

²² See Raimondo, Gina M. *The Honorable Gina M. Raimondo*. Interview by Reagan Foundation and Institute, January 26, 2024. <https://www.reaganfoundation.org/programs-events/webcasts-and-podcasts/podcasts/a-reagan-forum/the-honorable-gina-m-raimondo/>.

PILLAR 2: GLOBAL PEACE, STABILITY, AND SECURITY

GOAL	Impede Threats to the International Order, Defend Human Rights and Democratic Norms, and Stem the Proliferation and Delivery of Weapons of Mass Destruction	
STRATEGIC OBJECTIVES	2.1	Prevent, deter, and mitigate long-term risks
	2.2	Respond to emergent threats
	2.3	Support U.S. military superiority

The Challenge

The threat, misuse, and abuse of force by adversaries present a raft of national security concerns to the United States and to stability and security around the globe. The Department has a decades-long history of deploying its economic and regulatory tools to address these challenges. This was especially the case during the Cold War in support of arms control and non-proliferation and included many other goals to weaken the military threat posed by the Soviet Union. More recent examples include export controls issued in response to human rights violations in the PRC's Xinjiang region and the 2021 military coup in Burma.²³ The Department plays an important role in a whole-of-government approach to address all national security threats, not just commercial threats.

Today, the PRC poses the most complex, comprehensive, and serious challenges to U.S. national security. The PRC is building up and deploying its military in ways that undermine our security and the security of our allies and partners and the free flow of trade, as demonstrated by its growing military provocations in the East and South China Seas and in the Taiwan Strait.²⁴ It also seeks to dominate certain advanced technology sectors, especially AI, while using many of those technologies to advance its military modernization and fuel human rights abuses at home and abroad.²⁵ Russia's full-scale invasion of Ukraine, meanwhile, further highlights the threat authoritarian states across the globe pose to the established global order, as Russia also erodes long-standing commitments on arms control and nuclear non-proliferation. Other destabilizing military threats to U.S. national security, especially on issues related to non-proliferation and the facilitation of Russia's illegal war in Ukraine, include actions by pariah states such as North Korea and Iran.

²³ Bureau of Industry and Security. *Human Rights*. U.S. Department of Commerce. Accessed 2024. <https://www.bis.doc.gov/index.php/human-rights>.

²⁴ Raimondo, Gina M. *Remarks by U.S. Secretary of Commerce Gina Raimondo on U.S. Competitiveness and China*. U.S. Department of Commerce, November 30, 2022. <https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china>.

²⁵ *Ibid.*

Strategic Objectives

- 2.1 Prevent, deter, and mitigate long-term threats:** Proactively address threats to global peace, stability and security and deter adversaries from engaging in malign activities via cost imposition.
- 2.2 Respond to emergent threats:** Impede, monitor, and punish adversaries when imminent threats arise.
- 2.3 Support U.S. military superiority:** Enable the U.S. to maintain its military superiority by providing direct support; by promoting a strong and vibrant defense industrial base; and by enabling co-production with allies.²⁶

2.1 Prevent, deter, and mitigate long-term threats

Proactive measures help ensure that some threats never fully materialize in the first place, while delaying and mitigating the threats that do. Export controls, reviews by the Committee on Foreign Investment in the United States (CFIUS), outbound investment restrictions, commercial remote-sensing licenses, industry engagement, and international engagement all help by enabling us to get ahead of threats. The same can be said for participation in international standards-setting bodies. By guiding the commercialization of new technologies in a more secure and reliable direction, standards help to create a world in which certain risks are less likely to arise in the first place. And active U.S. participation in standards-setting bodies helps to ensure international interoperability, a level playing field for international trade, and leadership of U.S. firms in industries that are vital for our national security. In these ways, our support for foundational principles of standard-setting – such as transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and broad participation – also contributes to our national security objectives.

The Department also has many other tools to ward off potential threats. The International Trade Administration's (ITA) export promotion and commercial diplomacy initiatives, which aim to make the United States the economic partner of choice globally, reinforce the economic security of critical allies and partners by countering economic coercion and reducing dependence on strategic adversaries with U.S. investment, trade, and exports. Through our Commercial Law Development Program (CLDP), moreover, the Department provides government-to-government technical legal assistance to improve commercial legal frameworks and prevent instability in over 60 post-conflict and transitioning countries at their most vulnerable moments. NTIA also works toward a more stable world through its participation in the United Nations' International Telecommunication Union Development Sector's Partner2Connect initiative, which promotes global connectivity in developing nations.

²⁶ See BIS, *Guiding Principles*.

Furthermore, the Department promotes internationally recognized labor rights throughout the world, including by combatting forced labor through its participation in the Forced Labor Enforcement Task Force and training its Foreign Commercial Service officers to identify and respond to forced labor issues abroad.

Once threats do arrive on the horizon, the Department's regulatory authorities help deter and mitigate those threats through cost imposition. Export controls, tariff regimes, inbound investment review, and penalties signal U.S. credibility to malicious actors, such as in 2023 when the Department issued its largest standalone civil export control penalty in history of \$300 million. Deterrence is hard to observe because, when it succeeds, potentially harmful actions never occur, and there are an infinite number of non-actions. Even when an adversary takes a malicious action, deterrence is not an all-or-nothing proposition. Sometimes malicious actions are delayed, sometimes third countries will be deterred by observing penalties they are not party to, and sometimes actors who have already taken malicious action are deterred from taking further action. We cannot know the full breadth of the actions our policies have deterred. Nevertheless, when facing a threat, our highest priority is to deter an adversary from acting.

The Department also mitigates long-term risks after they arise. The Department continues to increase its involvement with State Department-led arms control and nuclear, chemical, and biological nonproliferation efforts by ensuring industrial compliance with various multilateral export control regimes, including the Australia Group (AG), Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement. BIS is also expanding its bilateral and plurilateral relationships with allies and partners worldwide to enhance and maintain stability in response to changing geopolitical and economic developments. These long-term regimes, in conjunction with established bilateral and plurilateral relationships, help prevent spiraling arms races between established powers. They also reduce the risk of dangerous items and technologies winding up in the hands of rogue states and nonstate actors who can be difficult, if not impossible, to deter.

2.2 Respond to emergent threats

When facing an imminent threat, such as PRC military modernization or Russia's full-scale invasion of Ukraine, the Department's tools impede adversarial action, monitor compliance with laws and regulations, and impose penalties for rule breaking. The Department impedes threats by strategically denying adversaries access to needed goods, U.S. investments, and U.S. expertise and markets. Export controls, which impose significant costs in terms of time and resources, are a significant tool in that toolkit. They help degrade or stall adversaries' military capabilities and widen the technology-military gap. Export controls are joined by the Department's work on inbound investment reviews as well as notification requirements and restrictions on outbound investment to impede misuse and abuse of U.S. goods, capital, markets, and intellectual property.

Although export controls often target the most critical technologies, strategic goods are not limited to these sensitive technology areas. Less sensitive commercial technologies can also be abused for regionally destabilizing conventional military activities, proliferating weapons of mass destruction, supporting terrorism, or violating human rights. A few examples are China's military-civil fusion strategy, its repression against minority groups, and Russia's use of U.S.-branded parts and components in unmanned aerial vehicles found on the battlefield in Ukraine. The Department's policies seek to halt the spread of these items just as with CET. But also, as with our approach to CET, we seek to impair adversary access to these technologies while avoiding unintended or counterproductive impacts on legitimate commercial and fundamental research activity.

2.3 Support U.S. military superiority

Ultimately, global peace, stability, and security cannot be ensured without strong U.S. armed forces. The Department directly supports the U.S. military in many ways. The Defense Department is the biggest federal customer for NIST's R&D efforts, spending tens of millions of dollars each year on multiple research projects and calibration services. NIST also conducts work for Defense Advanced Research Projects Agency (DARPA) to address many technical challenges, including the development and commercialization of chip-scale atomic clocks which can be incorporated into multiple weapons systems to provide resilience to GPS as well as supporting the Technologies for Heat Removal in Electronics at the Device Scale (THREADS) program. NOAA, meanwhile, provides significant imagery and data support for the military, in addition to personnel support, predictive weather and climate modeling, improved hazard assessments, resilience planning and institutional collaboration on issues including combatting IUU fishing, space, and the Arctic and Pacific. BIS-administered DPAS regulation is also a vital tool for all DOD procurement for the warfighter. DPAS, which is used by DOD at least 300,000 times per year, ensures that DOD's national defense programs are given priority within the U.S. industrial base to ensure timely delivery of industrial resources to support the readiness of the armed forces.

Additional to this direct support, the Department helps to ensure that U.S. armed forces maintain a durable military advantage over our adversaries. Export controls contribute directly to that mission by slowing the military modernization of our adversaries. ITA's Global Markets also leads the interagency Defense Advocacy Working Group (DAWG) to coordinate the government's defense-related trade advocacy work, in addition to embedding a commercial officer within the U.S. Indo-Pacific Command (INDOPACOM) to work on strategic commercial initiatives. BIS also has embedded personnel from INDOPACOM and U.S. Central Command (CENTCOM). Lastly, our domestic industrial policy, including CHIPS for America and EDA's Tech Hubs, aims to ensure our national defense has access to the technology it needs. Other tools to

support the defense-industrial base include trade missions, and supply chain analysis and Defense Production Act (DPA) surveys.

PILLAR 3:

CYBERSECURITY AND THE DIGITAL ECONOMY

GOAL	Maintain a Safe, Open, and Fair Digital Ecosystem	
STRATEGIC OBJECTIVES	3.1	Promote cybersecurity
	3.2	Advance U.S. values in the digital economy
	3.3	Foster ICT infrastructure resilience at home and abroad

The Challenge

The digital economy is the critical part of the economy that is facilitated through information and communications technology (ICT), including high and low technology software, hardware, mobile apps, networks, and services. The Bureau of Economic Analysis (BEA) estimates that in 2022 the digital economy accounted for \$2.6 trillion or 10.0% of U.S. GDP, growing at an average rate of 7.1% each year since 2017.²⁷ ICT underpins every sector and is a source of jobs, an enabler of global trade, and a key element of U.S. competitiveness.

Alongside these significant economic opportunities, ICT presents risks that must be prevented, mitigated, or managed effectively. Given the prevalence of ICT in government and critical infrastructure sectors and the use of ICT by nearly every American, adversarial access may not only compromise U.S. economic competitiveness, but U.S. national security as well. Major risks for the United States and our partners and allies include adversarial control over critical infrastructure, intellectual property theft, and adversary access to sensitive personal data (SPD).²⁸

Mirroring the growth of the digital economy, ICT risks and threats are increasing in frequency, sophistication, severity, and diversity. From spear phishing to data breaches, ransomware, and distributed denial-of-service (DDoS) attacks, malicious cyber activities are relentlessly ubiquitous. Foreign adversaries exploit vulnerabilities found in hardware and software, providing them with opportunities to cause harm, for instance, via access to SPD. These bad actors may selectively target individuals, corporations, critical infrastructure, and government assets. In addition to malicious cyber actors, foreign adversary control, by any means, over network infrastructure and services is a national security risk. Furthermore, SPD can be purchased from data brokers or accessed through other commercial means which can be used to harm or manipulate the American people and undermine our national security. Commercial transactions

²⁷ Bureau of Economic Analysis. *Digital Economy*. U.S. Department of Commerce. Accessed 2024. <https://www.bea.gov/data/special-topics/digital-economy>.

²⁸ SPD includes, for example, personally identifiable information (PII), insurance data, non-public electronic communications, consumer report data, identification card data, and data related to U.S. government employment and security clearances.

like these illustrate how malicious actors can not only specifically exploit trade to undermine security, but also generally how the digital economy increases threat vectors to Americans. The imperative to maintain a robust, secure, open, and competitive digital infrastructure – across all of society – is an urgent priority.

Strategic Objectives

- 3.1 Promote cybersecurity:** Cooperatively develop cybersecurity standards and best practices with industry, partners, and allies and promote widespread adoption.
- 3.2 Advance U.S. values in the digital economy:** Advance U.S. values, such as data privacy, security, and integrity; protect open data flows; and promote a safe, open, interconnected internet through advocacy, information sharing, and programmatic work.
- 3.3 Foster ICT infrastructure resilience at home and abroad:** Take protective action in response to threats, forecast ICT infrastructure disruptions from extreme weather, and invest in long-term resilience.

3.1 Promote cybersecurity

Strong cybersecurity practices help ensure that the United States continues to realize the full benefits of the 21st century digital economy and lead the world in innovation. To meet the needs of U.S. industry, federal agencies and the broader public, the Department develops and disseminates cybersecurity guidelines and best practices and conducts research to anticipate advances in technologies and future challenges. To stay at the cutting edge, in 2024 the Department updated its widely-used NIST Cybersecurity Framework to address the latest threats, working with the community to build a skilled cybersecurity workforce (including through NIST’s National Initiative for Cybersecurity Education (NICE)), developing cybersecurity guidance and standards to secure our software supply chain, and distributing these best practices to small and medium-sized enterprises (SMEs) through the Manufacturing Extension Program (MEP).

The Department promotes the adoption of these cybersecurity best practices at home and abroad, through industry and public engagement, educational initiatives, workforce development, diplomacy, and international standards bodies. In addition to advancing standards and research, the Department also boosts U.S. cyber leadership by promoting U.S. cyber companies in cyber trade missions and single company programs and works to counter cyber policies abroad that adversely impact U.S. companies and security, through commercial diplomacy, information sharing, and international institutions. Additionally, during CFIUS reviews, the Department advocates for stringent cybersecurity protections to address any cyber-related national security risks arising from a covered transaction. In these ways, the Department helps ensure individuals and public and private organizations across the globe

operate using commonly understood best practices, enabling greater opportunities for U.S. business abroad and a more stable international economy.

3.2 Advance U.S. values in the digital economy

The Department advances U.S. values in the digital order, such as the trusted free flow of data;²⁹ through advocacy and information sharing; through IP protection; through developing and sharing best practices for privacy and other digital issues, e.g. NIST's Privacy Framework; and by ensuring a safe, open, and interconnected internet. It does this, first, through formal programs with industry, bilateral dialogues, and in international fora. For instance, through NTIA's Communications Supply Chain Risk Information Partnership (C-SCRIP) program, the Department shares supply chain security risk information with at-risk small and rural U.S. communications providers and suppliers. We also work to promote cross-border data flows, frameworks for digital trade, and privacy best practices through the EU-U.S. Data Privacy Framework, our leadership in the Global Cross Border Privacy Rules System, and broader policy advanced through bilateral engagements and international organizations and initiatives, such as the International Telecommunications Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN), and the Declaration for the Future of the Internet (DFI).

The Department also advances U.S. values through its deep and unique relationships with industry and regular engagements with foreign governments, especially through its U.S. Commercial Service with trade experts in over 80 countries abroad and the USPTO's network of specialized IP attachés. These relationships open opportunities to share information and concerns on a more informal basis, through bilateral meetings, industry convenings, and more informal track 1.5 diplomacy with officials and non-governmental experts. They also enable opportunities to incentivize international behavior and promote trusted solutions and alternatives. They help shape the operating environment for the private sector, avoid more complex issues down the line, and give industry and governments the opportunity to act where needed. After coordinating with industry, for example, the USPTO provides guidance on IP and AI policy issues in international fora, including WIPO, IP5, OECD, the G7, and the G20. Finally, as arguably the world's largest producer of public data, the Department is uniquely positioned to promote data and information integrity and counter misinformation and disinformation, while also expanding open access to public data.

3.3 Foster ICT infrastructure resilience at home and abroad

To foster domestic ICT infrastructure resilience, the Department advises and takes protective action. The Department's primary regulatory tools to address concerning foreign adversary

²⁹ See Sullivan, *Remarks and Q&A on U.S.-China Relations*.

access to SPD and control of and access to U.S. ICT infrastructure are BIS's Office of Information and Communications Technology and Services (OICTS), and its participation in interagency inbound investment review mechanisms (CFIUS, Team Telecom).³⁰ To protect United States ICT from adversary access, the Department relies on its ICTS authorities to ban or mitigate certain types of transactions with a foreign adversary nexus in addition to issuing rules regulating foreign adversary ICT products and services. OICTS can proactively defend against foreign adversaries creating and exploiting vulnerabilities in key critical technology sectors that can be used against U.S. interests. Through its own investigations, referrals, and consultation, OICTS leverages public, proprietary, and national security information as well as its interagency partners in identifying gaps and weaknesses in the ICTS supply chain and issue rules that secure these transactions. And OICTS is working to prevent foreign malicious cyber actors from taking advantage of U.S. and allied Infrastructure-as-a-Service (IaaS) products to commit intellectual property and sensitive data theft, from engaging in covert espionage activities, and from threatening national security by targeting critical infrastructure.

The Department has other tools to promote ICT infrastructure resilience, too. CFIUS mitigates risk from foreign investments in U.S. firms that might result in foreign access to U.S. SPD and that raise national security concerns. Through its advisory role on Team Telecom, moreover, the Department weighs in on FCC license applications regarding foreign investment in U.S. communications infrastructure. And NIST's disaster and failure studies research helps develop and promote infrastructure resilience, while EDA's grant programs can help communities rebuild infrastructure following disasters to increase economic resilience.

The Department also contributes to U.S. ICT infrastructure resilience by forecasting extreme weather events. Space weather threatens space and ground-based technological systems through blackouts and failure in electricity transmission infrastructure. NOAA's Space Weather Prediction Center (SWPC) safeguards society with actionable space weather information, supplementing the work of its Weather Prediction Center (WPC) to forecast other extreme weather events that could impact ICT infrastructure. NOAA also supports the development of standards and best practices for space cybersecurity and conducts industry outreach to promote their widespread adoption.

The Department leverages other tools additional to its regulatory and forecasting authorities, including grant making, commercial diplomacy, and standards development. For many countries abroad, there are few good options for securing ICT infrastructure. To help bridge that gap, the Department's ten-year grant program, the Public Wireless Supply Chain Innovation Fund, funded by the CHIPS and Science Act and overseen by NTIA, works to catalyze the

³⁰ See, e.g., Executive Order No. 13,873. *Securing the Information and Communications Technology and Services Supply Chain*. Federal Register 84, no. 22,689 (May 17, 2019). <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>.

development and adoption of open, interoperable, standards-based networks by enabling trusted companies to compete in a market dominated by high-risk suppliers. This work complements the Department's participation in multilateral programs, such as the Digital Trade with Africa (DTA) Initiative, and Partnership for Global Infrastructure and Investment (PGI), a G7 initiative to facilitate hundreds of billions of dollars in public and private investment for low- and middle-income countries, partly in ICT networks and infrastructure. ITA also works with our partners and allies abroad on their 5G deployment strategies to advise and highlight a range of national security risks, including on building and maintaining ICT infrastructure. NIST, meanwhile, helps to foster ICT infrastructure resilience in the government itself by publishing Federal Information Processing Standards (FIPS) that are used by agencies across the federal government. Together, these many resources capture specific foreign products, services, investment, and persons that could present national security threats.

PILLAR 4:

CRITICAL SUPPLY CHAINS

GOAL	Build and Protect Resilient Supply Chains in Critical Sectors	
STRATEGIC OBJECTIVES	4.1	Analyze threats and develop policy solutions
	4.2	Inhibit adversaries from gaining strategic leverage
	4.3	Bolster affirmative alternatives

The Challenge

Global supply chains define the patterns of production, development, and movement of goods worldwide. Recent years have shown that disruption in one area — malicious or not — can ripple out across the globe. Concentration of a part or whole of a supply chain in the hands of a single country amplifies that risk.

All goods have supply chains. But not all supply chains are critical to national security. That depends on the good or the sector. The Department's national security work focuses on critical supply chains – or the supply chains that source key goods and sectors. That includes, for example, logistics services essential for the transport of goods; products necessary to support critical infrastructure, emergency response, and industrial bases; products for which disruption would cause mass panic or suffering; and other critical and essential goods and materials.³¹

The U.S. Government does not control global supply chains, as they result from voluntary transactions by private companies. But it can influence them to avoid “dangerous dependencies”:³² a reliance on products or sectors whose supply chains are particularly vulnerable to disruption due to market concentration or adversarial intent. Adversaries are constantly working to gain leverage over global supply chains. The PRC's decades-long initiative

³¹ This definition draws on guidance from Executive Order No. 14,017. *America's Supply Chains*. Federal Register 86, no. 11,849 (February 24, 2021). <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/> and Executive Order No. 13,953. *Addressing the Threat to the Domestic Supply Chain from Reliance on Critical Minerals from Foreign*. Federal Register 85, no. 62,539 (October 5, 2020). <https://www.federalregister.gov/documents/2020/10/05/2020-22064/addressing-the-threat-to-the-domestic-supply-chain-from-reliance-on-critical-minerals-from-foreign>.

EO 14017 does not precisely define critical supply chains but invokes various industrial bases (e.g. ICT, health, defense, etc.) and defines in section 6(b) these terms which are relevant for our needs: “Critical goods and materials” is defined as “goods and raw materials defined under statute/regulation as ‘critical’ materials, technology, or infrastructure”; “Critical minerals” as defined in EO 13953; “Other essential goods and materials” are defined in EO 14017 as “goods and materials that are essential to national and economic security, emergency preparedness, or to advance the policy set forth in section 1 of this order, but not included within the definition of ‘critical goods and materials.’” For instance, this includes (but is not limited to) software, steel, critical minerals and rare earths, pharmaceuticals, logistics, CET, food, critical infrastructure, and industrial base supply chains.

³² For “dangerous dependencies,” see Sullivan, *Sources of American Power*.

to establish chokepoint leverage in critical minerals supply chains illustrates that adversary advantage does not develop overnight but builds slowly over time, through a variety of means, including protectionist dumping, domestic subsidies, acquisitions and investments abroad, and attracting or stealing foreign expertise and trade secrets. But once established, adversary advantages can be quickly translated to economic coercion and malicious actions. The PRC's 2023 export controls on gallium, germanium, and graphite are prime examples of how a dangerous dependency on critical minerals can be weaponized to reduce access to key industrial inputs. In addition to malicious actions, unanticipated shocks, such as public health emergencies, logistical bottlenecks, conflict, and climate disturbances, can also create massive disruptions that can result in supply chain vulnerability.

The past few decades have shown that the market, especially when it is distorted by foreign subsidies, does not naturally adjust to address national security imperatives. Recent events have exposed structural weaknesses in the U.S. domestic industrial base and critical supply chains that support it – the result of underinvestment and preferencing outsourcing and offshoring over long-term security, sustainability, and resilience.³³ For instance, the vulnerabilities in semiconductor supply chains—which had accumulated over decades of inaction — were laid bare during the COVID-19 pandemic when automobiles sat on the assembly line and factories shut down because Americans did not have the chips to power the vehicles. And non-market actions by our adversaries—for example, the billions of dollars the PRC has devoted to producing legacy chips—can make it difficult to build supply chain resilience at home, as such actions erode U.S. and allied market share and undermine the commercial viability of U.S. and allied investments. When national security is at stake, we cannot defer to the invisible hand.

Strategic Objectives

- 4.1 Analyze threats and develop policy solutions:** Determine which supply chains across U.S. industry are most critical, evaluate their vulnerabilities, use quantitative and qualitative metrics to regularly assess and anticipate risk, and develop policy recommendations to prevent and respond to disruption.
- 4.2 Inhibit adversaries from gaining strategic leverage:** Counteract adversary influence by blocking strategic access.
- 4.3 Bolster affirmative alternatives:** Build critical supply chain resilience by reshoring and strengthening global partnerships.

³³ The White House. *Executive Order on America's Supply Chains: A Year of Action and Progress*. February 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf>.

4.1 Analyze threats and develop policy solutions

Rigorous data-driven analysis is key to proactively identifying critical supply chain vulnerabilities, anticipating national security risks, and developing policy solutions before and when a disruption occurs. This is the core mission of the Department's first-of-its-kind Supply Chain Center, housed in the Industry and Analysis unit within the International Trade Administration (ITA).³⁴ Launched in 2023, the Supply Chain Center, drawing on sector-specific experts in ITA, aims to be the analytic engine for supply chain resiliency policy for the U.S. Government. It helps to proactively strengthen critical supply chains and develop policy playbooks to mitigate risk and respond to shocks. The Supply Chain Center's work is complemented by the Industry and Analysis unit's CFIUS-specific supply chain methodology as well as other analysis and data collection across the Department, such as by the team of economists and data scientists in the Office of the Under Secretary for Economic Affairs (OUSEA), and through DPA surveys and ICT supply chain analysis by BIS. As arguably the world's largest publisher of public data, the Department also maintains an enormous range of open-source intelligence on industry, weather, oceans, and the environment that are increasingly used to inform this analysis. NOAA's vast data collection, for instance, provides critical ocean and weather intelligence for overseas, aviation, and road supply chains. NOAA also administers the Deep Seabed Hard Mineral Resources Act, which governs deep seabed mining activities by U.S. companies in areas beyond national jurisdiction, including for critical & rare minerals. The Department's many quantitative efforts are bolstered by qualitative feedback obtained through industry engagement and outreach to other stakeholders.

4.2 Inhibit adversaries from gaining strategic leverage

When confronting vulnerability, analysis must be followed by action. The Department protects U.S. critical supply chains to avoid and mitigate vulnerabilities by inhibiting adversary leverage. We do so primarily by impeding the many ways adversaries seek to gain strategic advantages along the supply chain by, for example, countering dumping and other unfair trade actions, protecting IP, blocking acquisitions and investments, prohibiting access to sensitive technologies, and protecting trade secrets and U.S. expertise. The Department must remain vigilant to the real threat posed by adversaries, especially the PRC, on critical supply chains. But we also must distinguish national security concerns from legitimate commercial activity. Too blunt a swipe risk doing more harm than good. For that reason, a tailored approach, which includes export controls, ICTS authorities, Section 232 tariff investigations, inbound investment reviews, and outbound investment restrictions and notifications, ensures that we do not

³⁴ International Trade Administration. *Remarks by Assistant Secretary Grant T. Harris at Supply Chain Summit "A Proactive and Strategic Approach to Supply Chain Resilience."* September 10, 2024. <https://www.trade.gov/feature-article/remarks-assistant-secretary-grant-t-harris-supply-chain-summit-proactive-and>.

unnecessarily burden dynamic and innovative supply chains as we protect our national security interests where we must.

4.3 Bolster affirmative alternatives

To prevent and respond to vulnerabilities, the Department also bolsters affirmative alternatives in critical supply chains, by helping to make more at home and partnering better abroad. Reshoring domestic production is a priority of the Biden-Harris Administration's modern industrial and innovation strategy, embodied by the 2022 CHIPS and Science Act. In doing so, it is critical to make full use of the resources and talent the United States has to offer. For example, minority business enterprises (MBEs) are not being effectively used to bridge critical supply chain disruptions. Making full use of U.S. industry would not only help protect national security but would also help to fill the \$6.3 trillion opportunity gap between minority and non-minority owned businesses.³⁵

Investing at home, however, does not imply an end to globally connected markets and supply chains. Nor does it mean that the government must pick winners and losers.³⁶ Instead, it enables private investment, strengthens trusted ecosystems, and builds inclusive growth. Beyond the semiconductor industry, EDA's Tech Hubs investments have the potential to further bolster supply chains across key critical and emerging technology sectors. Moreover, NIST's R&D efforts support long-term resilience by fundamentally altering the goods for which supply chains are required in the first place. For example, synthetic biology researchers may discover methods to replace existing production processes, such as for precursor materials, and to create new products entirely, resulting in new opportunities for diversifying production pathways and alleviating supply chain chokepoints.³⁷ These programs are also complemented by its trade missions, DPA authorities, community outreach programs, and its SelectUSA program, which has facilitated \$200 billion in foreign direct investment (FDI) in the United States since 2011 to attract foreign firms in critical sectors to establish production in the United States.³⁸

³⁵ Minority Business Development Agency. *All Minority Owned Firms Fact Sheet*. U.S. Department of Commerce, June 10, 2022. <https://www.mbda.gov/sites/default/files/2022-06/All%20Minority%20Owned%20Firms%20Fact%20Sheet%20-%20FINAL%206.10.2022.pdf>.

³⁶ Sullivan, *Remarks on Renewing American Economic Leadership*.

³⁷ The White House. *Bold Goals for U.S. Biotechnology and Biomanufacturing: Harnessing Research and Development to Further Societal Goals*, 27. March 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/03/Bold-Goals-for-U.S.-Biotechnology-and-Biomanufacturing-Harnessing-Research-and-Development-To-Further-Societal-Goals-FINAL.pdf>.

³⁸ U.S. Department of Commerce. *U.S. Commerce Department Announces \$200 Billion Milestone in Foreign Direct Investment Under Secretary Raimondo*. January 25, 2024. <https://www.commerce.gov/news/press-releases/2024/01/us-commerce-department-announces-200-billion-milestone-foreign-direct>.

Not all products or sectors are appropriate for reshoring, however. The Department also has other tools to counteract dangerous dependencies. Strengthening global partnerships is crucial. Partnering with likeminded nations to strengthen shared and trusted supply chains (friendshoring) not only helps us build more resilient supply chains, but also leads to greater progress and prosperity.³⁹ That is the logic underlying the Department's participation and leadership in the supply chain pillar of the Indo-Pacific Economic Framework for Prosperity (IPEF). In strengthening these global partnerships, the Department draws not only on its DC-based industry experts, but also on its extensive network of trade experts serving in over 100 cities in the United States, and 80 posts around the world as members of the U.S. and Foreign Commercial Service and as USPTO attachés. In addition to promoting friendshoring, the Department also encourages bringing supply chains closer to home, further diversifying supply chains elsewhere in the world, and identifying viable supply chains for substitute goods.

Each of these options has variable tradeoffs, including dependability, quality, and potential cost impacts to industry and consumers. In each case, the Department applies the appropriate policy tool to resolve any potentially dangerous dependencies with minimum collateral impact.

³⁹ U.S. Department of Commerce. *Indo-Pacific Economic Framework for Prosperity Pillar II: Supply Chains*. September 7, 2023. <https://www.commerce.gov/sites/default/files/2023-09/2023-09-07-IPEF-Pillar-II-Final-Text-Public-Release.pdf>.

PILLAR 5: SAFE ENVIRONMENTS

GOAL	Advance Climate Security, Protect Space Commerce, and Support Safe Oceans and Sustainable Fishing	
STRATEGIC OBJECTIVES	5.1	Build climate resilience and promote climate solutions
	5.2	Support a safe and secure operating environment for space commerce
	5.3	Ensure safe oceanic and Arctic navigation and combat IUU fishing

The Challenge

Droughts, fires, hurricanes, and rising sea levels are just a few of the acute consequences of climate change, which are increasing and intensifying at an alarming rate. Even gradual changes can wreak havoc on natural resources, food supplies, and supply chains – leading to diverse problems including political instability, mass migration, food insecurity, and death. Together, these impacts are costly to mitigate, harmful to life and property, and threatening to critical infrastructure and the life-sustaining needs of society. They also impact our military’s ability to respond, maintain superiority on the battlefield and protect U.S. interests abroad.

Climate change also opens up new vectors of competition and vulnerabilities. As the Arctic Sea ice melts, for instance, geopolitical competition around resources, territories, and transportation routes could rise. Safe oceanic navigation, especially in the polar north, is critical to avoiding escalatory accidents, executing search and rescue operations, and addressing emergent threats. Climate change also exacerbates the threat of illegal, unreported, and unregulated (IUU) fishing by shifting fish stocks, disrupting trade, and incentivizing fishers to break the rules.

Threats in the natural world are not limited to climate change. In space, there are many other challenges. For instance, coronal mass ejections from the sun – expected to cyclically peak between 2024-2025 – produce changes in space weather that threaten critical infrastructure. The thousands of commercial satellites orbiting Earth risk collision, spraying debris across the outer atmosphere and jeopardizing space-based critical infrastructure. Lastly, the nature of space systems and their reliance on information systems and networks put a premium on strong cybersecurity protections, U.S. commercial space leadership, and countering malign intent.

Strategic Objectives

- 5.1 Build climate resilience and promote climate solutions:** Mitigate and adapt to climate change through monitoring, emergency response, innovation and IP protection, and the development of decision-relevant environmental intelligence, data, and models to build resilience.
- 5.2 Support a safe and secure operating environment for space commerce:** Promote space cybersecurity, ensure U.S. commercial space leadership, prevent in-space collisions, and develop a robust space weather prediction system.
- 5.3 Ensure safe oceanic and Arctic navigation and combat IUU fishing:** Support safe oceanic and Arctic navigation with ocean intelligence and sea ice products and services, and combat IUU fishing through monitoring, law enforcement, and tech assistance.

5.1 Build climate resilience and promote climate solutions

The Department's response to climate change must be both reactive and proactive. Climate change is a reality. Adapting to and reducing its impact is an imperative, not a choice. At the Department, this happens by building data-driven resilience. The Department's immense data collection, predictive modeling, and analysis — undertaken by NOAA, Census, BEA, OUSEA, and ITA — provides decision-makers across the public and private sectors with critical, actionable climate data to inform their decisions.⁴⁰ The Department has cutting-edge data-gathering capabilities, such as NOAA's Geostationary Operational Environmental Satellites (GOES), which provide advanced imagery and atmospheric measurements of Earth's Western Hemisphere, real-time mapping of lightning activity, and improved monitoring of solar activity and space weather. Such data helps decision-makers prepare for and respond to extreme weather events and gradual changes in climate. They provide a foundation for resilience research, measurement, and guidance that the Department leverages in industry convenings and commercial diplomacy abroad. They also feed the Department's direct work with coastal communities, such as NOAA's Climate-Ready Coasts and Communities Initiative.⁴¹ They also inform the Department's many disaster recovery, emergency response, and community resilience resources, funding, and services at EDA, NIST, NTIA, and NOAA.

Solutions to mitigate and adapt to the most severe impacts of climate change require immediate action coupled with long-term planning. The Department promotes climate solutions first by incentivizing and protecting innovation to accelerate the development and

⁴⁰ Commerce Department, *Strategic Plan*, 42.

⁴¹ National Oceanic and Atmospheric Administration. *NOAA and the Inflation Reduction Act*. U.S. Department of Commerce. Accessed 2024. <https://www.noaa.gov/inflation-reduction-act>.

commercialization of key climate technologies, such as through USPTO's Climate Change Mitigation Pilot Program and Patents for Humanity Clean Energy Technologies awards competition, EDA's Tech Hubs, and SelectUSA's mission to attract FDI in the U.S. It also helps to commercialize climate and clean technologies, actively promotes U.S. exports of those technologies, and offers technical and legal assistance to partners and allies to help achieve climate goals under the Paris Agreement.

5.2 Support a safe and secure operating environment for space commerce

The Department's tools to protect against malign intent in space include export controls, the conditioning of operations of remote sensing systems for the protection of national security interests, and the promotion of cybersecurity norms. Certain spacecraft items require authorization for export, reexport, or transfer, including transferring registration, control, or ownership of certain spacecraft to certain foreign persons or countries. Commercial remote-sensing licensing is another regulatory tool, overseen by the recently reorganized and elevated Office of Space Commerce (OSC) at NOAA, to condition the operation of remote sensing systems when those operations yield commercial remote sensing data both unique to the United States and posing national security concerns. Additionally, USPTO is collaborating with the National Aeronautics and Space Administration (NASA) to ensure its space-related IP is protected, as well as working with Artemis Accord partners to emphasize the importance of IP protection related to space innovation. Beyond these authorities, the Department promotes strong cybersecurity norms in the space commerce industry through industry convenings and diplomatic engagement.

Especially in the case of licensing conditions, restrictions on space businesses must be weighed against the strategic goal of U.S. commercial space leadership.⁴² U.S. commercial space leadership ensures national security objectives by maintaining a domestic industrial base with the technological capability to meet the highest military and intelligence needs. In the case of remote sensing satellites, NOAA's operating restrictions are limited to the most sensitive systems and are temporary in nature, in order to prevent an erosion of U.S. industrial leadership over time. As additional actions are considered, the Department should continue to evaluate the impacts of short-term Department actions on industry and long-term national security objectives.

Malign intent is not the only threat in space. Unintended collisions of orbiting objects not only threaten other space systems, but also the Earth-based infrastructure that relies on space-

⁴² See Graves, Don. *Remarks by Deputy Secretary of Commerce Don Graves at Satellite 2023 Government and Military Forum*. U.S. Department of Commerce, March 14, 2023. <https://www.commerce.gov/news/speeches/2023/03/remarks-deputy-secretary-commerce-don-graves-satellite-2023-government-and-military-forum>.

based systems. The expansion of space commerce heightens this risk. To address it, NOAA is developing the Traffic Coordination System for Space (TraCSS), a modern, public-private system that provides space situational awareness (SSA) data and space traffic coordination safety services to space operators, free of charge with open data sharing.

5.3 Ensure safe oceanic and Arctic navigation and combat IUU fishing

Reliable data are critical to safe navigation. NOAA's data, mapping, and forecasting ensure that oceans are safe to navigate, protecting against unintended accidents, collisions, and other dangers. In the Arctic, navigation challenges increase in complexity and severity, due to harsher weather conditions, more limited satellite coverage, and presence of ice. To address those problems, NOAA's sea-ice products, data, and services contribute to better domain awareness.

Furthermore, IUU fishing threatens national security by undermining human rights norms, depleting fish stocks, harming ocean health, and destabilizing food systems and ecosystems around the world.⁴³ The Department's tools to combat IUU fishing include a mixture of monitoring, law enforcement, and technical assistance. The Department's actions contribute to more sustainable use of oceans, fewer labor abuses, and stability of fish stocks worldwide.

⁴³ See National Security Memorandum 11. *Combating Illegal, Unreported, and Unregulated Fishing and Associated Labor Abuses*. Federal Register 87, no. 38,693 (June 27, 2022). <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/27/memorandum-on-combating-illegal-unreported-and-unregulated-fishing-and-associated-labor-abuses/>.

GOING FORWARD

Our nation faces a rapidly evolving threat landscape, characterized by rising geopolitical tensions with our adversaries and the unprecedented pace of technological change. This shift has dramatically transformed the strategic environment. As a result, our national and economic security are increasingly intertwined, and the Department plays an expanded role in national security policymaking.

This strategy, designed to facilitate institutional adaptation at the Department, helps to set issue priorities and strategic direction on national security issues, align messaging, “connect the dots” across bureaus, and grow a culture that prioritizes national security within the Department. However, there is more work to be done. Meeting this moment requires a proactive, whole-of-government approach to support ongoing collaboration and new efforts to address emerging threats. To accomplish the strategic objectives set out in this strategy, the Department and our partners in government should prioritize the following.

Targeted Investment

To maintain global leadership, we must innovate more and innovate faster than the rest of the world. The Department should therefore double down on the Biden-Harris Administration’s historic, targeted investments — through programs such as CHIPS for America, Tech Hubs, the Public Wireless Supply Chain Innovation Fund, and the Build Back Better Regional Challenge — to support scaling critical and emerging technologies like AI, biotechnology, quantum information science, and clean energy technology. Increased R&D investment and support should also be a priority.

Increased Departmental Capacity and Resources

The Department faces increasingly wide and complex demands related to our national security mission. Meeting those demands will require new funding, legal tools, and hiring authorities. The Department should prioritize obtaining the resources and authorities to hire staff with increased technical expertise and high-level security clearances, and to secure additional Sensitive Compartmentalized Information Facility (SCIF) space for classified work. In addition to increasing the Department’s internal capacity, we should also prioritize investment in high-quality data that our partners in government and the private sector can leverage.

Enhanced Coordination within the Department and across the U.S. Government

Given the Department’s increased role in national security policymaking, there is an urgent need for greater strategic coordination and engagement on national security issues. This strategy highlights many Department initiatives that intersect with our national security objectives — including research, commercialization, domestic investment, protecting America’s innovations,

and supporting the private sector — and opportunities for further internal collaboration in a few key areas. It also provides insight for other U.S. government agencies in and our partners in Congress into how the Department can support Administration-wide national security goals, particularly in the interagency process.

Deepen Engagement with Industry Partners and Allies

To address global challenges that threaten U.S. economic prosperity — such as supply chain disruptions, climate change, unfair trade practices, and aging infrastructure — we must deepen our engagement with like-minded allies and industry partners. That includes encouraging innovative cooperation through plurilateral agreements like IPEF. It also includes seeking international coordination to establish trusted technology ecosystems and enhance protection and enforcement protocols, such as by updating the Department’s export controls and enforcing new outbound investment restrictions. Private sector engagement — including the Department’s work to advance international standards that are aligned with our nation’s values and promoting their widespread adoption — are similarly vital.



U.S. Department of Commerce

1401 Constitution Ave NW
Washington, DC 20230

commerce.gov

