DHS STRATEGIC ACTION PLAN TO COUNTER THE THREAT POSED BY THE PEOPLE'S REPUBLIC OF CHINA

Defending the Homeland in the Era of Great Power Competition

Homeland Security

U.S. Department of Homeland Security
Office of Strategy, Policy, and Plans

Contents

With honor and integrity, we will safeguard the American people, our Homeland, and our values.

Executive Summary

Though the global security environment has evolved considerably since the Department of Homeland Security's (DHS) founding, its fundamental mission has endured: To safeguard the Homeland, its values, and the American way of life. The changing geopolitical landscape, led by the return of great power competition, is nowhere more evident than in the People's Republic of China's (PRC) ascension to the world-stage.

For decades, marked by Beijing's symbolic entry in the World Trade Organization (WTO), the PRC has leveraged non-traditional tools to gain access to and exploit our global institutions and rules-based order, with little to no response. This has resulted in the erosion of, and direct attacks against, U.S. national security and economic competitiveness, including the exploitation of our immigration system manipulation of open-markets, and theft of our intellectual property. Under this Administration, the PRC's threat to the Homeland is now being appropriately prioritized and met with a resolute commitment to safeguard America.

As denoted in the 2017 National Security Strategy of the United States (NSS) and 2020 United States Strategic Approach to the PRC (Strategic Approach), DHS and the broader United States Government (USG) have entered into a period of sustained competition against the PRC, requiring continued attention, adaptation, and resourcing to safeguard the American people and Homeland.

The American people rely on DHS to play an integral role in the USG's competition with the PRC. The more than 240,000 men and women of the Department stand ready to curb malign PRC activity and the myriad of other challenges. This study, which seeks to more strategically identify, assess, and leverage the Department's unique resources and authorities, reflects these efforts.

The DHS China Strategic Action Plan (SAP) is informed by and nests within the NSS and the Strategic Approach, which delineate the United States' strategic approach to PRC through the pursuit of four goals: (1) protecting the American people, the Homeland, and the American way of life; (2) promoting American prosperity; (3) preserving peace through strength; and (4) advancing American interests.

BORDER SECURITY AND IMMIGRATION

DHS recognizes that the protection of the American people requires a border that is secure and an immigration system that is fair and anchored in American values. For far too long, these processes have been exploited to the detriment of American workers and small and medium-sized U.S. businesses. The Department, led by U.S. Customs & Border Protection (CBP), U.S. Immigration & Customs Enforcement (ICE), and U.S. Citizenship & Immigration Services (USCIS), has and will continue to augment immigration vetting and monitoring, including for student and tourist visas, and will return PRC visa-overstays who continue to undermine visa integrity.

TRADE AND ECONOMIC SECURITY

America's global leadership is underpinned by a free-market environment that cultivates unprecedented opportunity and innovation at home. Through nefarious trade tactics—including intellectual property theft, piracy, and counterfeiting—the PRC undermines American prosperity and competitiveness. With the increasing ubiquity of e-Commerce transactions and proliferation of counterfeits, the Department's mission to enforce trade rules and protect economic prosperity and public safety remains more important and, arguably, more challenging than ever.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

In an increasingly digital and interoperable world, we face expanding threats to our cyber networks and critical infrastructure in scope, scale, and frequency. The Department's Components, led by the Cybersecurity and Infrastructure Security Agency (CISA), are acutely aware of these risks, particularly those emanating from the PRC. While CISA plays a central and cross-cutting role across our Nation's critical infrastructure, the Transportation Security Administration (TSA) and U.S. Coast Guard (USCG) also play a key role in bolstering resilience to cyber and emerging technology vulnerabilities in the transportation sector.

MARITIME SECURITY

A secure maritime domain at home is predicated on coordinated operations that leverage the authorities and partnerships of our maritime partners abroad. The USCG and CBP provide a strong maritime security presence that reinforces U.S. sovereignty and builds international coalitions to strengthen global norms and protect the rules-based order. .

The PRC Threat to the Homeland

Beijing's ultimate objective, as Acting Secretary Wolf stated in his 2020 State of the Homeland, is clear: to leverage "every aspect of its country, including its economy, its military, and its diplomatic power, demonstrating a rejection of Western liberal democracy and continually renewing its commitment to remake the world order in its own authoritarian image."

As the COVID-19 pandemic has demonstrated, Beijing's activities have and, if left unchecked, will continue to have direct, palpable, and reverberating impacts on the security and prosperity of the Homeland, our citizens, and our values. This threat does not stem nor derive from the Chinese people, but rather the Chinese Communist Party's (CCP) consolidation of power and policies it has propagated in its rule over mainland China. This threat is complex and multifaceted: one that is economic, geopolitical, and ideological.

OPPOSING IDEOLOGIES

The CCP ideology and political principles are diametrically opposed to those of the United States of America. Rooted in authoritarianism, the CCP continues to engage in predatory economic behavior abroad and widespread repression at home. Under the CCP, the PRC protects and advances the party's interests, and those of other global authoritarian regimes, to the detriment of political, religious, and civil liberties and diversity, targeting some of the country's most vulnerable populations. Since General Secretary Xi Jinping assumed power, these concerning trends have only worsened.

Conversely, the United States is anchored in freedom and openness, affording citizens political liberty, unrivaled business opportunity, religious freedom, the rule of law, and societal openness—exemplified by the right to peacefully dissent and protest. These coveted rights are fiercely protected and viewed as fundamental strengths in the Homeland.

THE NEW BATTLEFRONT: GREY ZONE TACTICS (ECONOMIC ESPIONAGE AND FINANCIAL TRANSACTIONS)

Rather than leverage conventional weapons like bullets and tanks, the PRC continues to employ non-traditional tactics that it has calculated will reap maximum gain without

eliciting significant U.S. response. These include the continued exploitation of our immigration system, free-market economy, and culture of innovation and openness. The costs to our economy and values are palpable and pervasive, resulting in trillions of dollars of lost revenue, millions of lost jobs[1], and a lasting deleterious impact on American prosperity.

PRC malfeasance, deception, economic exploitation, and intimidation delayed global recognition of and sabotaged the response to COVID-19, thereby causing mass death and economic destruction in the Homeland and beyond. And while the regime in Beijing criminalized fentanyl in 2019, it failed to adequately address illicit supply chains originating in the PRC's chemical industry, which transit precursor chemicals through drug cartels and other transnational criminal organizations. The result is that chemicals and drugs originating in China infiltrate U.S. communities as finished synthetic opioids, fueling the Homeland's opioid crisis. This directly contributed to nearly 71,000 U.S. overdose deaths in 2019.[2]

Economic Prosperity Under Assault

Innovation and economic ingenuity, bedrocks of American global competitiveness, are under attack. The PRC regime's predatory economic practices, including rampant intellectual property theft, counterfeiting and piracy, and deflated commodity prices—made possible in part using forced labor—erode this strength, costing American jobs and decimating entire industries and towns throughout the United States. Moreover, these pernicious activities wreak long-lasting damage upon the economic prospects as well as the health and welfare of Americans.

Exploitation of the U.S. Immigration System

The PRC abuses our immigration system and exploits U.S. businesses and academic institutions to obtain access to cutting-edge American technology and information. By illicitly acquiring proprietary information, the PRC undermines American prosperity, our scientific and technological competitiveness, and—ultimately—the safety of our armed forces and the American people. These exploitative acts advance the CCP's interests while adversely impacting the students, visitors, and workers seeking entry for legitimate purposes that benefit themselves and meaningfully contribute to the Homeland.

1. "2020 Special 301 Report", United States Trade Representative, April 2020, https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf.
2. "Drug Overdose Deaths in the United States, 1999-2019," National Center for Health Statistics, Centers for Disease Control and Prevention (CDC), https://www.cdc.gov/nchs/products/databriefs/db394.htm.

Threats to our Elections and Other Critical Infrastructure

Beijing intensified its influence efforts ahead of the 2020 U.S. elections to shape the U.S. policy environment, sway political figures it viewed as antithetical to its interests, and deflect and counter PRC-related criticisms. These pernicious efforts have the potential to deny Americans the fundamental right to make electoral decisions free from nefarious influence. Additionally, Beijing continues to threaten American national security, economic security, and public health and safety through deliberate efforts to surveil and target the functions, systems, and assets—physical and virtual—of U.S. critical infrastructure,[3] upon which all Americans depend.

Supply Chain Vulnerabilities

The promise of access to Beijing's expansive market has drawn U.S. businesses to the PRC. Decisions that appear advantageous to individual businesses in the short term can put the company, its clients, and the Nation at risk. Overdependence on a supplier country that can manipulate prices and drive free-market competitors out of business makes the Homeland and the American people vulnerable. As other competitors are eliminated, disproportionate amounts of U.S. medical supplies, technology, and electronics, including the critical minerals used to manufacture them, become concentrated under the control of a country that has a history of waging economic warfare to achieve political goals in peacetime.

Data Collection

If oil was the commodity synonymous with the industrial age, data is the coveted resource of the digital age.[4] The PRC is increasing its efforts to consolidate global data collection as part of an ongoing, comprehensive effort designed to build its economic strength and shape international information flows in line with its geopolitical and security interests. Technology like Unmanned Aerial Systems (UAS) and telecommunications systems that serve as vectors for information collection are cases in point. The consolidation of data in PRC possession, much of which is obtained without informed consent, will accelerate the proliferation of data-centric technologies that threaten the privacy of U.S. citizens, undermine American prosperity, and empower digital authoritarianism.

3. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

4. PRC National Information Center, March 10, 2020.

THE DEPARTMENT'S UNIQUE ROLE

DHS is uniquely positioned to play a more pronounced and expansive role in USG efforts to confront the PRC in a geopolitical environment where insidious tactics continue to be Beijing's weapon of choice. The Department's mission-set is both broad and unique. It is charged with administering both the USG's most long-standing mandates, such as travel and trade facilitation, while concurrently performing its new missions like cyber counter-espionage and blunting misinformation. We stand ready to leverage our unique authorities and resources to curb the generational threat posed by the PRC.

Meeting the PRC Threat to the Homeland

To more holistically catalogue DHS's current operational posture regarding the PRC, Acting Secretary Wolf directed the creation of an intra-DHS China Working Group. This section reflects a key Working Group output, intended to augment the Department's threat mitigation posture. DHS has worked and continues to work with public and private partners, both domestically and internationally, to combat all threats to the United States, including those posed by Beijing.

DHS activities are delineated in four areas: (1) Border Security and Immigration; (2) Trade and Economic Security; (3) Cybersecurity and Critical Infrastructure; and (4) Maritime Security.

BORDER SECURITY AND IMMIGRATION

A free and fair immigration system, bolstered by strong and secure borders, is critical to advancing the goals of the NSS and the Strategic Approach.

Screening and Vetting

A critical pillar of the Department's immigration mandate is CBP's immigration screening, vetting, and monitoring operations, which focus on curbing the PRC's exploitation of our systems through the immigrant or non-immigrant visa processes, or via border crossings. CBP's capacity to perform these functions rests on the invaluable work of the National Targeting Center (NTC). In conjunction with Department of State's (DoS) Bureau of Consular Affairs, the NTC conducts analysis to track high-risk travelers from the PRC. This includes implementing Presidential Proclamation 10043, Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China

(Presidential Proclamation 10043), who present a high risk of obtaining critical or sensitive information to advance the PRC's Military-Civil Fusion (MCF) Strategy.[5]

USCIS, in coordination with ICE and CBP, continues to safeguard American values, evidenced by its recent issuance of policy guidance to ensure immigrant visa applicants affiliated with a Communist or totalitarian party, including the CCP, are not granted lawful immigration status. USCIS is also focused on closing security gaps in the immigration investment (EB-5) program, which some PRC nationals exploit to steal intellectual property and exert nefarious influence on American companies.

PRC Immigration Violators

The PRC's disrespect for U.S. law and international norms is evidenced by its refusal to cooperate with DHS to accept the return of approximately 40,000 PRC nationals who have overstayed or violated their visa or status conditions (and are subject to final orders of removal from the United States). Beijing's refusal to cooperate forces ICE to release hundreds of PRC nationals, many with convictions for violent crimes, into American communities, jeopardizing public safety and visa integrity.

Operation Fox Hunt

ICE continues to curb a covert PRC government effort known as Operation Fox Hunt, through which Beijing targets and seeks to repatriate and prosecute PRC individuals living in foreign countries whom the PRC alleges have committed crimes under PRC law. These efforts often use unsanctioned or illegal tactics to surveil, threaten, and harass Chinese citizens as well as American citizens and lawful permanent residents living in the United States.[6]

Drug and Human Trafficking

CBP and ICE's Homeland Security Investigations (HSI) unit continue to detect, deter, disrupt, and dismantle PRC-based transnational criminal organizations' (TCO) penetration of illicit networks within the Western Hemisphere to traffic fentanyl, illicit drug precursors, and other harmful substances endangering U.S. communities via the Southwest border, international mail shipments, and express consignment operations.

CBP is committed to implementing STOP Act[7] regulations, which will augment the

5. Military-Civil Fusion (MCF) is a national strategy of the CCP to develop the People's Liberation Army (PLA) into a "world class military" by 2049. Under MCF, the CCP is acquiring the intellectual property, key research, and technological advances of the world's citizens, researchers, scholars, and private industry in order to advance the CCP's military aims. The CCP is systematically reorganizing the PRC science and technology enterprise to ensure that new innovations simultaneously advance economic and military development (https://www.state.gov/military-civil-fusion).

Department's ability to prevent PRC-based TCOs from exploiting the U.S. Postal System to flood American communities with fentanyl and other deadly substances.

TRADE AND ECONOMIC SECURITY

DHS plays an important role in facilitating and safeguarding American trade and commerce. At its core, this mission is focused on facilitating lawful trade while protecting U.S. innovation and American workers.

Counterfeit, Forced-Labor, and Pirated Goods

CBP and ICE HSI continue to protect U.S. businesses and communities from counterfeit, forced labor-made, and pirated import flows emanating from China. These products undercut competitively produced goods, reinforce a forced labor system that contradicts American values, and pose a health and safety risk to millions of Americans nationwide (e.g., faulty airbags, defective toys, substandard medical equipment, etc.).

Additional trade enforcement efforts include CBP's work to interdict PRC commodities produced with forced labor where Beijing continues to inhumanely detain Uyghurs and other vulnerable minorities.[8] In Fiscal Year 2020, CBP issued an unprecedented 8 Withhold Release Orders (WROs) against goods from China to prevent the importation of key products made with forced labor, including cotton, hair products, textiles, and computer parts. These inhumane practices are not only antithetical to unalienable rights and an abdication of the PRC's international commitments, they also undercut competitively priced goods from domestic manufacturers relying on lawfully-compensated labor instead of slavery.

Through its leadership at the National Intellectual Property Rights Coordination Center (IPR Center) and work at the Cyber Crimes Center (C3), HSI coordinates USG efforts to combat trade fraud and IP violation investigative operations that safeguard the health and safety of the United States public, the economy, and our military. The IPR Center, and other DHS stakeholders, led the Operation Stolen Promise effort, a USG initiative to criminally investigate the people and organizations perpetrating COVID-19-related fraud and criminal activity (fraudulent, counterfeit or prohibited PPE, pharmaceuticals, and test-kits).

6. See https://www.justice.gov/opa/pr/eight-individuals-charged-conspiring-act-illegal-agents-people-s-republic-china.

7. The Synthetics Trafficking and Overdose Prevention Act (STOP) of 2018 establishes requirements related to U.S. Postal Service (USPS) international mail shipments. Among other requirements, the bill requires USPS to gather advanced data on its shipments and share such information with U.S. Customs and Border Protection and assesses a fee on overseas inbound express mail.

8. Since at least 2017, the PRC continues to detain more than one million Uyghurs, ethnic Kazakhs, ethnic Kyrgyz, and members of other Muslim minority groups in internment camps designed to eradicate detainees' cultural and religious identities, and to indoctrinate them with CCP ideology. In these camps, there is extreme overcrowding, sleep and food deprivation, medical neglect, physical and psychological abuse, and forced labor, amongst other mistreatment.

Intellectual Property Rights Protection

ICE and CISA also continue working on the front lines to support companies, academia, and State, Local, Tribal and Territorial (SLTT) partners with intellectual property theft deterrence, prevention, mitigation, and response. The HSI-led Export Enforcement Coordination Center (E2C2) is a vital interagency outfit that further curbs the illicit transfer of sensitive, export-controlled U.S. military and dual use articles, services, and technology from U.S. industry.

The close and continued partnership with private (industry, academic institutions, etc.) and public stakeholders [at the Federal, State, Local, Tribal and Territorial (FSLTT), and international allies], is integral to the Department's trade enforcement mission. For instance, HSI's IPR Center outreach initiative, Operation Joint Venture, shares information with public and private sectors to combat the illegal importation and distribution of counterfeit, substandard, and tainted goods.

CBP also deploys robust enforcement efforts against Antidumping and Countervailing Duty evasion. Last year alone, CBP prevented $287 million in duties from being evaded, of which 90 percent were connected to manufacturers in China.

Supply Chain Security

COVID-19 has also spotlighted adversaries' potential weaponization of U.S. supply-chain dependencies. The internal DHS Trade & Economic Security (TES) Policy Council[9] has been instrumental in developing industrial policy expertise to address trade asymmetries, such as PRC efforts to dominate critical technologies and target U.S. vaccine research. The National Risk Management Center (NRMC) has also been at the forefront of assessing key supply-chain dependencies of critical infrastructure.

With 90 percent of U.S. imports and exports traveling through the Marine Transportation System (MTS), supply chain resiliency is inextricably linked to the USCG's charge of protecting lawful commerce, both in our waterways and on our seas.[10] This includes addressing growing concerns of Illegal, Unreported, and Unregulated (IUU) Fishing worldwide, as reflected in the release of the USCG IUU Fishing Strategic Outlook (Outlook). The Outlook charts a strategic vision to curb

9. TES is a sub-element of the DHS Office of Strategy, Policy, and Plans.

10. Maritime Trade constitutes $5.4 trillion of annual commerce and supports 23 million American jobs. The importance of maritime trade in global commerce is reflected in the USCG Maritime Commerce Strategic Outlook, which prioritizes facilitating secure waterway trade and travel.

these illicit activities.

Malign Foreign Investment and Business

The Department continues to protect the Homeland from nefarious cross-border investment, providing sound national security guidance on foreign business transactions involving U.S. businesses and U.S. telecommunications. DHS plays an active role in the Committee on Foreign Investment in the United States (CFIUS) and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom).

In June 2020, DHS played a leading role in recommending to the Federal Communications Commission to grant in part and deny in part the Pacific Light Cable Network (PLCN), a high-capacity undersea cable connecting Hong Kong to the Homeland, which would prevent it from making landfall in Hong Kong while permitting it to connect the United States to the Philippines and Taiwan. This recommendation to deny in part sought to prevent Beijing's efforts to create an Information and Communications Technology (ICT) infrastructure hub that would jeopardize the privacy of U.S. persons as well as U.S. national and economic security.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

DHS remains focused on working with stakeholders to protect the cyber and physical elements of the nation's critical infrastructure, including those sectors most frequently targeted by the PRC.[11]

Collaboration with Industry, FSLTTs, and international partners

CISA maintains a close and collaborative partnership with industry tailored to bolstering cyber-mitigation practices against adversaries, from nation- and non-state actors alike. This unique private sector partnership approach enables CISA to disseminate cyber-threat information, host trainings and personnel exchanges, and circulate threat bulletins and alerts. Recent products have included spotlighting PRC-affiliated cyber threat actors targeting U.S. government agencies, PRC malware variants used to attack and maintain a presence on U.S. victim networks, as well as targeting and attempted network compromise of healthcare, pharmaceutical, and research sectors working on the COVID-19 response and vaccines.[12]

Additionally, CISA actively participates in the protection of federal networks from

11. Critical Manufacturing, Defense Industrial Base, Energy, Healthcare and Public Health, Transportation, Information Technology, Communications, and Government Facilities to include the Education and Election Infrastructure subsectors.
12. For additional information, please visit https://us-cert.cisa.gov/china.

malign cybersecurity actors, including those emanating from the PRC. This includes leveraging EINSTEIN systems and other technology, like Continuous Diagnostics Mitigation, to support federal civilian agencies to better manage cyber risks. CISA also engages directly with impacted industry and SLTT stakeholders, deploying Cyber Hunt and Incident Response Teams to identify, contain, and deny adversarial activity and develop mitigation plans for the removal and remediation of cyber threats.

CISA's work also extends to SLTTs. To counter Russian and PRC efforts to influence American electoral processes, CISA strengthened its partnerships with local election leaders across the country to ensure our elections are safe and secure. This includes supporting state and local election officials' efforts to secure their systems, including offering services like Remote Penetration Testing, Risk and Vulnerability Assessments, ongoing Vulnerability Scanning, and incident response. In addition to helping secure election systems, CISA supports election officials' efforts to reduce the risk of mis-, dis-, and mal-information (MDM) to the election.

Internationally, CISA continues to engage with like-minded allies to emphasize the need for security and integrity in 5G technology. With the signing of The Prague Proposals, an agreement on securing 5G global deployment, CISA will continue to prioritize 5G and ICT supply-chain risks into its discussions with global counterparts, with a particular focus on the Western Hemisphere, to catalyze trusted vendor innovation and foster a safer and more secure global cyber-ecosystem.

Other DHS Components, such as ICE and U.S. Secret Service (USSS), remain focused on the core tenets of the Department's cybersecurity mission, supporting U.S. companies as well as domestic and international partners, to combat cyber-crime. For example, HSI developed Operation Red Umbrella, a multi-pronged strategic action plan to combat China Supported Operations (CSO) related criminal activity to subvert U.S. customs and immigration laws.

Bolstering Transportation Security

The PRC continues to present a persistent threat to the Homeland's transportation infrastructure. TSA and USCG are expanding their capabilities to address PRC threats to the transportation sector, with dedicated ongoing efforts looking specifically at cyber threats to the pipeline, aviation, and maritime subsectors. To help integrate these DHS-wide efforts and better partner across the interagency, the Secretary created a Joint Cyber Coordination Group (JCCG) within DHS headquarters. The JCCG serves as a

focal point for DHS components to support cross-departmental awareness, planning, and operational response options for the Secretary.

Information and Communications Technology (ICT) Mitigation

CISA is continuing to take important steps to secure our ICT, and, in particular, to secure next generation telecommunications equipment and software. The NRMC continues to promote secure and resilient domestic 5G deployment by leading efforts to identify, analyze, prioritize, and manage these risks. This includes the development of products, including a "5G repository" to identify and educate partners of trusted telecommunication vendors. This work is particularly important and timely, given the PRC's passage of its National Security Law, which Beijing has indicated it will exploit as a means to collect information from PRC-produced equipment, PRC citizens, and/or PRC firms.

MARITIME SECURITY

The Department, led by the USCG, is taking proactive measures to ensure a freer and more prosperous Homeland. As 90 percent of our nation's imports and exports move through the MTS, which directly or indirectly supports 23 million American jobs, U.S. security and prosperity is inextricably linked to the maritime domain.

Ports and waterways, both at home and abroad, depend on complex networks of organizations and information, operational, and navigational technologies, such as satellite navigation, satellite communication, wireless communication, and the Automatic Identification System (AIS), that are critical to MTS functionality. The size and significance of the MTS continue to make it an attractive target for cyber threat actors. Driving a robust defense of MTS systems and networks, including protection against cyber domain challenges, must remain among the nation's top priorities.

The continued enforcement of fair, honest, and open competition for MTS services is also vital. By reinforcing these global norms and bolstering our partner nations' ability to deter global malign maritime activity, DHS is securing the Homeland while supporting Department of Defense (DoD) activities in the Indo-Pacific and the Arctic.

The USCG's current maritime security activities include its campaign to counter the scourge of IUU fishing; improving maritime security in Oceania, the Caribbean, and the coasts of Africa and South America; supporting DoD South China Sea regional security; and curbing PRC influence operations in the Arctic. These efforts will counter our adversaries' exploitative activities that undermine the maritime rules-based order, jeopardize food access and availability, destroy responsible economies, and ultimately

Continuing to Protect the Homeland

The Department recognizes and anticipates a sustained and enduring competition against the PRC. DHS understand that its policies, programs, and operations will require continued adaptation, calibration, and coordination with key stakeholders to address the full spectrum of PRC threats to the Homeland. The continued optimization of these policies and plans, as detailed in the following section, necessitates ongoing planning, both today and in the years to come.

This section outlines the Department's prospective commitments, pursuant to the NSS and the Strategic Approach, which are delineated into four lines of effort: (1) Border Security and Immigration, (2) Cybersecurity and Critical Infrastructure, (3) Trade and Economic Security, and (4) Maritime Security.

BORDER SECURITY AND IMMIGRATION

The PRC's manipulation of the U.S. immigration system has cost jobs and undermined our values as a free, open, and meritorious society.

Although DHS has made substantial progress in stemming this threat, significant work remains. The following actions reflect the Department's continued commitment to curb the PRC threat by bolstering our border security and committing resources to detect and disrupt PRC efforts to abuse our immigration system.

1. Ensure the Effective Removal of PRC Nationals from the United States

At present, approximately 40,800 PRC nationals in the United States are subject to final orders of removal. Despite a proclaimed commitment to address this national security threat and adhere to international norms, the PRC has ignored more than 1,300 ICE requests for travel documents since October 2017. Consequently, ICE has been forced to release more than 1,000 PRC nationals from custody, many with convictions for violent or other serious crimes.

DHS will continue efforts to ensure the PRC accepts the timely removal of its nationals subject to final orders of removal from the United States. As Beijing continues to

flout its international obligations and disrespect U.S. law, DHS will continue to seek escalated consequences—including visa restrictions.

2. Increase Screening and Vetting of PRC Visa and Immigration Benefits Applications

DHS is taking immediate action to identify and implement additional screening and vetting actions in response to PRC non-traditional collectors and other malign actors seeking to exploit the U.S. immigration system to steal intellectual property and obtain a competitive advantage. These actions include:

- Electronic Visa Update System (EVUS) Expansion: DHS will enhance EVUS data collection and sharing, which will bolster the U.S. Government's ability to address national security, counterintelligence, public safety, and fraud concerns.
- Strengthening the STEM Operational Practical Training (OPT) Program: The OPT program is a type of work authorization that allows participants to gain experience in their field of study after they have completed an academic program. ICE, in conjunction with relevant DHS components, will assess the efficacy of the OPT program and provide recommendations to the Secretary to bolster security processes where appropriate.[13]
- Increasing Vetting of Certain PRC Students and Researchers in High-Risk Fields: ICE will conduct an assessment to identify additional measures to increase vetting of a sub-set of MCF-affiliated PRC students, researchers, and workers in high-risk fields.
- Enhancing Security Measures During the Immigration Benefit Adjudication Process: In coordination with relevant DHS offices, USCIS is enhancing adjudication processes, which are critical to ensure improved vetting and investigation of PRC nationals applying or extending their stay to work or study in fields that contribute to the PRC's MCF strategy.
- Identifying Additional U.S. Visa Categories Vulnerable to PRC Exploitation: DHS, in conjunction with relevant agencies, will identify nonimmigrant and immigrant visa categories susceptible to exploitation by non-traditional collectors and accordingly enhance scrutiny of PRC nationals seeking these benefit categories.

13.This includes evaluating the current list of "areas of study" that qualify a foreign national for STEM OPT and take appropriate safeguards to prevent the transfer of sensitive technology and intellectual property.

- Expanding Visa Data Sharing Efforts: DHS will work to enhance the functionality and interoperability of vetting systems and databases across the interagency, which will include securing increased funding through a "term fee" charge (done so via statutory change). This will expand the Department's threat picture and ability to more holistically track nefarious PRC-directed actors, both at the border and at their source.
- Collaborating with Partners: DHS will lead efforts, in collaboration with relevant agencies, to share information with like-minded partners related to PRC nationals subject to Presidential Proclamation 10043. This information exchange will help to inform partners' own visa adjudications, based on responses, and provide DHS critical feedback to inform internal enforcement efforts.
- Legislative Proposal to Enhance the Integrity of Immigration Benefit Programs: While employment and investment-based immigration benefit programs (e.g., EB-5 Immigrant Investor Program) stimulate the U.S. economy through capital investment and job creation, the PRC continues to exploit these programs for malign purposes. USCIS will work with relevant congressional stakeholders to propose legislative language to augment immigration benefit integrity.

3. Optimize Law Enforcement Coordination

Curbing PRC's Uncoordinated Law Enforcement Activity

To mitigate the threats posed by the PRC government's continued uncoordinated law enforcement activity in the United States, including Operation Fox Hunt efforts, DHS will build on recent successes and:

- Continue HSI efforts with the Federal Bureau of Investigations and the Diplomatic Security Service to investigate individuals who support Operation Fox Hunt efforts in the United States.
- Advance and strengthen existing intelligence-based targeting programs to identify PRC-affiliated operatives traveling for nefarious purposes.
- Closely track PRC-owned or affiliated vessels entering or exiting the Homeland.

Dismantling PRC Illicit Pathways to the Homeland

China-based TCOs leverage tools, networks, and underground banking schemes and

14. Components will further share relevant job aids, targeting rules, and methodologies with Five Eyes partners to identify PRC non-traditional collectors.

cryptocurrencies, including repatriation of proceeds from illicit activity in the U.S. market, to facilitate the illicit arrival of PRC nationals and narcotics.[15] To address this concerning trend, DHS will continue to:

- Map networks facilitating the illicit arrival of PRC nationals at the U.S. Southwest Border to identity opportunities for DHS leadership engagement to mitigate risks on direct flights between the PRC and Mexico.
- Identify opportunities to interdict, investigate, and ensure prosecution of PRC-based TCOs and other PRC malign actors facilitating the illicit introduction of fentanyl and other dangerous narcotics into American communities. Where appropriate, DHS will collaborate with relevant agencies to leverage existing relationships with PRC law enforcement to achieve these goals.
- Methamphetamine Lessons-Learned Study: DHS will conduct a "lessons learned" exercise on illicit distribution of methamphetamine precursors from the PRC entering the United States to inform DHS's continuing efforts to interdict fentanyl precursors from PRC.

4. Identify PRC Human Rights Abusers

Denying Entry to Human Rights Abusers

The PRC continues to carry out a campaign of repression in Xinjiang, targeting Uyghurs, ethnic Kazakhs, ethnic Kyrgyz, and members of other ethnic and religious minority groups.[16] DHS will continue to identify human rights abusers and, where possible, make recommendations to DoS to revoke visas or otherwise deny entry to PRC officials complicit in these heinous acts. Additionally, DHS will support interagency efforts with third countries to highlight the PRC's human rights abuses—especially as the PRC takes a seat on the United Nations Human Rights Council. This effort converges with action plans to identify areas where goods produced with forced labor are entering the U.S. supply chain.

TRADE AND ECONOMIC SECURITY

Although the tools have evolved, the PRC's objective remains unchanged: undermine our competitiveness, a core strength that advances American prosperity.

15. In Fiscal Year (FY) 2019, CBP encountered over 3,000 PRC nationals attempting to enter the United States illegally, including over 2,000 PRC nationals encountered along the U.S. Southwest Border.

16. Specific abuses include mass arbitrary detentions, severe physical and psychological abuse, forced labor and other labor abuses, oppressive surveillance used arbitrarily or unlawfully, religious persecution, political indoctrination, forced sterilization, and other infringements of the rights of members of those groups in Xinjiang.

From facilitating shipping since the Nation's founding and now e-Commerce in the digital age, protecting legitimate commerce remains at the core of the mission of homeland security. The Department's core trade enforcement components, coupled with recent policy and risk assessment installations like CISA's NRMC and PLCY's Trade & Economic Security team, are focused on protecting these vital interests, both today and in the decades to come.

1. Bolster the DHS Trade & Economic Security Mission

DHS TES helps to coordinate, distill, and formulate policy concepts and positions governing trade enforcement and facilitation, foreign investment risk management, supply chain risk management, international free trade agreements, and enhanced engagement with critical infrastructure and industrial sectors. As the November 2020 report of the Homeland Security Advisory Council (HSAC) made clear, it is critical for the Department to institutionalize its economic security mission.

Formalization of the Economic Security Framework (ESF)

DHS PLCY will work with Congress to formalize (in statute) the production of an Annual Assessment of the Economic Security of the Homeland, with a near-term focus on understanding risks posed by the PRC and threat-mitigation opportunities. The ESF is intended to identify and prioritize national and economic security risks as well as to assess and articulate prospective supply-chain risks.[17]

2. Quantify and Catalogue PRC State-Owned Enterprise (SOE) Behavior

PRC SOE Trends/Risk Approach

DHS PLCY, in coordination with Components and the interagency, will conduct a study to more comprehensively understand, assess, and articulate common behaviors, drivers, and trends of PRC SOE behavior, particularly in regions of growing concern, such as Central and South America; identify PRC SOE nefarious behavior, where possible; and create a comprehensive risk assessment approach that will then be applied to scope top PRC SOE threats by sector. The study will encompass a risk analysis, identification of trends/indicators, and summation of top 10 most concerning PRC SOEs.[18]

17. This report would mirror the statutory requirement, pursuant to title 10 United States Code (U.S.C.), section 2504, requiring DoD to submit an annual report summarizing DoD industrial capabilities-related guidance, assessments, and actions contained in the NDAA for FY 2012.
18. PRC SOEs will be selected from previously selected NDAA (1999) Section 1237 "Communist Chinese Military Companies" list, Department of Commerce, Bureau of Industry and Security (BIS) "Entity List", Department of Justice indictment, or those which have been sanctioned by the Department of Treasury Office of Foreign Assets Control (OFAC).

3. Combat PRC Forced Labor

Forced Labor U.S. Supply Chain Assessment

DHS, in coordination with the intelligence community and National Security Council, will conduct an assessment examining the extent to which goods produced using forced labor are imported to the United States. Subsequent activities will include messaging, engagements, and discussions with industry counterparts.

Engagement with International Partners

DHS PLCY, in coordination with CBP, ICE, and DOS, will present the above findings and engage allies and multilateral organizations, such as the WTO, World Customs Organization, Organization for Economic Cooperation and Development, and the Universal Postal Union. DHS will also identify lessons learned and encourage likeminded partners to conduct similar assessments to determine the pervasiveness of PRC-coordinated forced labor in the global supply chain.

4. Mitigate PRC Exploitation of Critical Technologies

DHS Supply Chain Coordination

DHS PLCY will incorporate lessons learned from existing interagency risk assessment processes (such as CFIUS and Team Telecom) and implement HSAC recommendations to develop best practices for supply chain-focused interagency entities—including, as applicable, the Federal Acquisition Security Council (FASC).

5G Lessons Learned

DHS will develop a 5G "Lessons Learned" policy paper with recommendations to the Secretary for options to more proactively identify and mitigate risks posed by high-risk PRC products and emerging technology within ICT and other critical U.S. supply chains.

Semi-Conductor/Chip Assessment

DHS TES, in coordination with relevant DHS equities and the Department of Commerce, will draft a policy paper outlining options the USG can execute to expand trade with fledgling chip sectors and like-minded economic partners, including India and Taiwan.

5G Lessons Learned

DHS will develop a 5G "Lessons Learned" policy paper with recommendations to the Secretary for options to more proactively identify and mitigate risks posed by high-risk PRC products and emerging technology within ICT and other critical U.S. supply chains.

Semi-Conductor/Chip Assessment

DHS TES, in coordination with relevant DHS equities and the Department of Commerce, will draft a policy paper outlining options the USG can execute to expand trade with fledgling chip sectors and like-minded economic partners, including India and Taiwan.

5. Strengthen Messaging of PRC Impact on Homeland

Expanding Awareness of PRC Predatory Economic Behavior

In coordination with the Department of Commerce, DHS will sponsor a nationwide public engagement plan to educate small and medium-sized businesses about the PRC's predatory economic behavior – to include forced labor, IP theft, counterfeiting, free-trade fraud, and dumping, as well as identification and mitigation approaches.

National Public Awareness Campaign

DHS will develop a proposal for a national-level public awareness campaign focused on articulating the personal privacy, economic, and safety risks of disclosing information to untrusted data-service companies or platforms. The proposal will use the Department's "Blue-Ribbon" campaign as a template.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

In the modern age, safeguarding the Homeland's critical infrastructure and cyberspace is as necessary and complex as any USG mission. DHS continues to closely monitor cyber espionage and non-traditional intelligence collection efforts against intellectual property and personally identifiable information (PII). The Department also remains increasingly concerned with the PRC's ability to disrupt U.S. critical infrastructure, including pipelines, for days to weeks.[19]

Although recent actions have mitigated the PRC's attempts to dominate global 5G market share, Beijing continues to threaten and disrupt critical infrastructure, posing

19. Worldwide Threat Assessment, ODNI Director Daniel Coats (January 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

new challenges to U.S. national security, privacy, and resistance to malign influence. Exponential increases in internet speed, connectivity, and productivity likewise increase the risks of PRC operations against the Homeland. DHS has a unique and important role to play in curbing these malign activities.

To bolster these capabilities, DHS will:

1. Prioritize Operational Efforts to Counter Malicious PRC Activity

Expand DHS-wide Cyber Resilience

DHS will expand efforts that leverage the capabilities of DHS Components (including CISA, TSA, USCG, USSS and ICE HSI) to protect U.S. critical infrastructure, federal civilian government networks, and the American people from malicious cyber activity originating from the PRC and to establish resiliency within DHS critical systems from potential cyber-attacks.

Leverage Joint Cyber Coordination Group (JCCG)

DHS will leverage the JCCG to align cross-Component efforts and help prioritize ongoing interagency efforts to counter the PRC's malicious cyber activity and efforts to target critical infrastructure.

Enhance Marine Transportation System Cyber Assessments

USCG Cyber Protection Team (CPT) will accelerate international and domestic cyber assessment and threat hunting missions to detect, deter, and prevent nation-state actors from impacting critical infrastructure associated with the MTS. USCG CYBER will explore mechanisms to identify potential CPT deployments in support of maritime critical infrastructure.

Expand Global Partnerships

DHS and its interagency partners will seek support from Congress to increase capacity building efforts such as provision of training to key regional and global partners. This will include expanding cybersecurity technical assistance and capacity trainings to the Indo-Pacific region and beyond.[20] It will also encompass workshops on optimizing public-private cooperation, cyber hygiene, and workforce development.

Cyber Response Options

DHS will develop courses of action to deter and respond to malicious PRC cyber

20. Technical assistance and trainings include cyber vulnerability workshops, Cyber Hunt and Incident Response Trainings, and Advanced Cybersecurity exercises.

activity, such as imposing scalable costs.

Safeguard UAS Information

DHS will form an internal working group, led by DHS PLCY, to understand the risk of information theft from UAS and identify mitigation opportunities for DHS Secretary consideration.

2. Enhance Public-Partner Engagement Across the 16 Critical Infrastructure Sectors[21]

Expand Briefs to Partners

CISA will enhance public-private engagement by establishing recurring PRC-threat briefings through CISA's regional and field presence.

Optimize Threat Information-Sharing Coordination

DHS will formulate a PRC information-sharing coordination campaign focused on synchronizing products, PRC-specific intelligence briefings, and collaborative planning with the National Infrastructure Protection Plan (NIPP) Partnership sector and cross-sector groups via the Critical Infrastructure Partnership Advisory Council (CIPAC). This campaign will include responses to threats against the education sector and other pertinent sectors.

Bolster Cloud Provider Protection

DHS will collaborate with industry and interagency partners to protect cloud and other infrastructure service providers from PRC attack through national policy, legislation, and public awareness campaigns.

3. Increase Resilience of the Homeland to Nation-State Threats

Critical Infrastructure Assessment

DHS PLCY will bring together FEMA, CISA, and other key DHS Components to understand the potential impacts associated with PRC threats to critical infrastructure and assess any gaps in current DHS National Preparedness and Planning activities.

Expand Homeland Partner (FSLTT and Private Sector) Threat Trainings and Exercises

CISA and FEMA will augment cyber and physical trainings and exercises with FSLTT

and industry partners to strengthen the resilience of critical infrastructure targeted by the PRC. This includes incorporating PRC Tactics, Techniques, and Procedures (TTPs) and other "real-world" nation-state scenarios into large-scale cyber exercises, including Cyber Storm VII and Cyber Storm VIII.[22]

4. Assess the Need for Establishment of a Bioeconomy Critical Infrastructure Sector or Subsector

Bioeconomy Sector

Working through the National Infrastructure Protection Plan (NIPP) partnership, DHS will explore the utility of creating a new critical infrastructure sector or subsector with associated Sector-Specific Agency and councils for assets, systems, data, databases, networks, and other elements within the United States (e.g., "bioeconomy critical infrastructure").

5. Engage with Academic Community about PRC Threat

Intra-DHS Academic Coordination Group

DHS will develop an intra-DHS Academia Coordination Working Group (Working Group) to engage academic stakeholders, particularly universities with sensitive information or intellectual capital and property. The Working Group will also develop an assessment of academic stakeholders' awareness of cyber vulnerabilities and identify areas to improve DHS-Academic collaboration.

MARITIME SECURITY

DHS will advance a whole-of-government effort to defend U.S. national interests in the maritime domain and promote economic prosperity through enhanced engagement with like-minded nations and key maritime stakeholders. In addition to the cyber threats discussed above, DHS will do this through the following objectives: (1) uphold and enforce U.S. laws; (2) safeguard American interests in the Arctic and Sub-Arctic Regions; (3) strengthen allies and partnerships at home and abroad; and (4) advance a free and open Indo-Pacific and global commons.

1. Uphold and Enforce U.S. Laws

Augment Information Sharing

Bolster information-sharing and collaboration, as well as processes across the DHS

enterprise to combat human smuggling and labor trafficking and to increase awareness and field operations efforts. This includes, for instance, standardizing criminal indicators and questions for various operations (IUU fishing, Darkweb) across multiple DHS Components and mission-sets (e.g., ICE HSI and USCG).

2. Safeguard American Interests in the Arctic and Sub-Arctic Regions

Advance DHS Arctic Cooperation and Collaboration

USCG will augment the development and deployment of maritime domain awareness technologies (e.g., manned and unmanned aviation assets) and surface presence capabilities, namely a robust icebreaking fleet, in the Polar regions. Additionally, the USCG will continue to invest in logistics and personnel support to enable enhanced operations, increased presence, and engagement to bolster allied collaboration and counter PRC's growing influence and ambitions as evidenced in Polar Silk Road efforts.[23]

3. Strengthen Partnerships (at Home and Abroad)

Maritime Threat Information-Sharing

Expand maritime threat and domain awareness information-sharing arrangements with Indo-Pacific partners, for example, by increasing cooperation with the Philippines.

Protect the Integrity of International Fora

DHS and USCG will increase their participation in the Arctic Council and the Arctic Coast Guard Forum (ACGF) to counter attempts to gain access to and influence these, and other, international bodies.

Law Enforcement Support to Regional Partners

CBP will seek collaboration with DoS Bureau of Narcotics and Law Enforcement Affairs (INL) and DoD Indo-Pacific Command (INDOPACOM) to assist regional customs enforcement outfits. This will seek to expand collaboration with Laos' Investigative Suppression Division (ISD), for instance, to counter drug-smuggling and wildlife and human trafficking.

4. Advance a Free and Open Indo-Pacific and Global Commons

Partnership Identification (Asset/Operations and Information-Sharing)

USCG will leverage its assets, operations, and information-sharing agreements

with identified priority partners, including activities listed in the Oceania Regional Engagement Plan (REP) to counter PRC maritime threats.[24]

Academic Partner Cooperation

USCG will enhance academic collaboration with Pacific Island Nation allies, including hosting Coast Guard (or Coast Guard equivalent) students at maritime law enforcement institutions of higher learning, including the U.S. Coast Guard Academy and the Maritime Law Enforcement Academy (MLEA).

Advantage at Sea Strategy Implementation

Identify areas to synchronize the "Advantage at Sea" strategy[25] to further leverage concurrent USCG efforts that counter malign and coercive PRC activities, which include IUU fishing.

Conclusion

The United States faces a new period of long-term competition with the People's Republic of China. The growing threats from the PRC cause new risks to the American people, the Homeland, American security and prosperity, and the American way of life. DHS is prepared to meet these challenges. At the same time, DHS is receptive to constructive, results-orientated engagement, including cooperation from the PRC where our nations' interests coincide.

The Department will continue to respond relentlessly to the threat posed by Beijing, consistent with the National Security Strategy and the Strategic Approach—including through appropriate operational direction to DHS components.

Homeland Security

WITH HONOR AND INTEGRITY, WE WILL SAFEGUARD THE AMERICAN PEOPLE, OUR HOMELAND, AND OUR VALUES

www.dhs.gov