

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

June 21, 2024

The Honorable Pete Buttigieg  
Secretary  
U.S. Department of Transportation  
1200 New Jersey Ave. SE  
Washington, D.C. 20590

Dear Secretary Buttigieg:

The Committee on Oversight and Accountability (Committee) is investigating the Chinese Communist Party's (CCP or the Party) aggressive use of disintegration warfare tactics,<sup>1</sup> including economic warfare, cyber warfare,<sup>2</sup> and supply chain interdiction,<sup>3</sup> to disrupt and capture our nation's critical maritime and transportation networks and infrastructures. Indeed, CCP attacks on these critical networks and infrastructures are a direct threat to America's national security and economic strength.<sup>4</sup>

National security officials are reportedly alarmed by "[t]he intrusion of Chinese hackers into US maritime and transportation networks," and believe that these "hackers are there not to collect intelligence but to potentially cripple computer networks in the event of a U.S.-China conflict."<sup>5</sup> As recently as April 18, FBI Director Christopher Wray warned that the People's Republic of China (PRC) "has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America's will to resist."<sup>6</sup> Director Wray also explained that "[t]he FBI worries what this sprint means for our country's critical infrastructure, since 'these vital sectors—everything from water treatment facilities and

---

<sup>1</sup> See Andrew J. Bilden, *China is Competing for U.S. Allies, Too*, U.S. Naval Inst. (Dec. 2018).

<sup>2</sup> Sam Sabin, *Top U.S. officials warn Congress of China's hacking powers*, Axios (Jan. 31, 2024) ("This is a world where a major crisis halfway across the planet could well endanger the lives of Americans here at home through the disruption of our pipelines... [and] the crippling our transportation modes.").

<sup>3</sup> See Trevor Phillips-Levine, *The Art of Supply Chain Interdiction: To Win Without Fighting*, War on the Rocks (May 26, 2023).

<sup>4</sup> See Stephen Weber, *Threats to America's critical infrastructure are now a terrifying reality*, The Hill (Feb. 11, 2024).

<sup>5</sup> Sean Lyngaas & Evan Perez, *FBI and Justice Department use court order to try to disrupt Chinese hacking targeting key us infrastructure*, CNN (Jan. 31, 2024).

<sup>6</sup> *Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says*, Fed. Bureau of Invest. (Apr. 18, 2024).

energy grids to transportation and information technology—form the backbone of our society.”<sup>7</sup>

The Committee is investigating what the Department of Transportation (Department or DOT) is doing to stem the tide of the CCP’s relentless and bold attacks on our nation’s critical maritime and transportation networks and infrastructures. DOT has important responsibilities to protect America and its citizens from the CCP’s economic warfare intended to destroy our national security and economic prosperity.

### Broader Committee Investigation

The Committee is conducting oversight of the federal government’s work to protect the American people from CCP political warfare<sup>8</sup> and nefarious influence operations. For decades, the CCP has sought to infiltrate and influence every aspect of American society.<sup>9</sup> The CCP’s goal is plain: defeat the “main enemy,” which counterintelligence officials have identified as America.<sup>10</sup> The fronts are multiple; according to the CCP itself: “[t]he battlefield will be everywhere.”<sup>11</sup> And the tools are myriad, with the “united front”<sup>12</sup> leading as one of the PRC’s<sup>13</sup> “magic weapons,”<sup>14</sup> as described by General Secretary Xi Jinping,<sup>15</sup> to advance the Party’s aim of global domination.<sup>16</sup> United front work (UFW), which may be executed by the United Front Work Department (UFW) or elsewhere in the Party, is a “unique blend of engagement, influence activities, and intelligence operations” that the CCP uses to “influence other countries’ policy toward the PRC and to gain access to advanced foreign technology.”<sup>17</sup> UFW “generally

---

<sup>7</sup> *Id.*

<sup>8</sup> “Political warfare seeks to influence emotions, motives, objective reasoning, and behavior of foreign governments, organizations, groups, and individuals in a manner favorable to one’s own political-military objectives.” Mark Stokes, *The People’s Liberation Army General Political Department: Political Warfare with Chinese Characteristics*, Project 2049 Inst. (Oct. 14, 2013).

<sup>9</sup> See generally Constantine C. Menges, *China The Gathering Threat* (2005); H.R. Rep. No. 105-851 (1999) (“Cox Report”); Robert Spalding, *War Without Rules* (2022); Col. Grant Newsham, *When China Attacks: A Warning to America* (2023); Kerry K. Gershaneck, *Political Warfare: Strategies for Combating China’s Plan to “Win without Fighting”* (2020); see also Larry Diamond and Orville Schell, *China’s Influence & America’s Interests: Promoting Constructive Vigilance*, Hoover Inst. (2019).

<sup>10</sup> Menges, *supra* note 9; Gershaneck, *supra* note 9 (“The PRC is engaged in war against the United States. It is not mere competition or malign influence, but war by PRC definition.”); Newsham, *supra* note 9, at 60 (The CCP “seeks global domination” and “will fight its main enemy, the United States, to achieve it.”).

<sup>11</sup> Qiao Liang & Wang Xiangsu, *Unrestricted Warfare: China’s Master Plan to Destroy America* (PLA Lit. & Arts Pub. House 1999) (China) (military colonels describing twenty-four varieties of warfare).

<sup>12</sup> “While the CCP’s United Front Work Department has functional responsibility for these [warfare] operations and activities, PRC united front work is a task of all CCP agencies and members.” Gershaneck, *supra* note 9, at 22.

<sup>13</sup> It is essential to understand that Xi Jinping has removed any “veneer of separation between the [CCP] and the Chinese state.” Gershaneck, *supra* note 9, at 43 (quoting Ann-Marie Brady, *Exploit Every Rift: United Front Work Goes Global*, in David Gitter et al., *Party Watch Annual Report*, Ctr. for Adv. China Res. (2018)).

<sup>14</sup> Ann-Marie Brady, *Magic Weapons: China’s political influence activities under Xi Jinping*, Wilson Ctr. (Sept. 18, 2017); see also Sel. Comm. on the Chinese Communist Party, *Memorandum: United Front 101*, at 7 (“United Front 101 Memo”).

<sup>15</sup> Alex Joske, *The party speaks for you: Foreign interference and the Chinese Communist Party’s united front system*, Austl. Strategic Pol’y Inst. (June 9, 2020) (quoting Xi Jinping at 2015 Central United Front Work Meeting).

<sup>16</sup> See, e.g., Newsham, *supra* note 9, at 43 (“The People’s Republic of China may settle for dominance rather than occupation, but it does indeed aim to rule us all.”).

<sup>17</sup> United Front 101 Memo, *supra* note 14, at 1.

involves covert activity and is a form of interference that aids the CCP's rise."<sup>18</sup> United front "networks" are used "to carry out relationship-focused influence campaigns through a multitude of proxies."<sup>19</sup>

Despite years of false promises to the West, the CCP openly seeks to achieve its destructive ambition. In 1999, two People's Liberation Army Air Force colonels authored *Unrestricted Warfare*, which has been described as a strategic military vision for the PRC to defeat America through political warfare.<sup>20</sup> Retired Brig. Gen. Robert Spalding, who has served in senior positions in strategy and diplomacy with the U.S. Departments of Defense and State for decades, characterizes the book as "the main blueprint for China's efforts to unseat America as the world's economy, political, and ideological leader," which "shows exactly how a totalitarian nation set out to dominate the West through a comprehensive, long-term strategy that includes everything from corporate sabotage to cyberwarfare to dishonest diplomacy; from violations of international trade law and intellectual property law to calculated abuses of the global financial system."<sup>21</sup> Kerry Gershaneck, former counterintelligence officer who wrote a seminal book on combatting PRC Political Warfare, has explained that *Unrestricted Warfare* details CCP use of "any methods" where "the boundaries between war and non-war and between military and non-military affairs [have] systemically broken down."<sup>22</sup> To successfully combat these highly organized and pervasive warfares spawned by China, federal agencies must first recognize and understand them.

The CCP "know[s] the strength of the American people, of the American idea, and that's why China has launched so many warfares to try to weaken us, divide us, and get us to hate ourselves and each other."<sup>23</sup> Retired Col. Grant Newsham, former U.S. Marine Liaison Officer to the Japan Ground Self-Defense Force and U.S. Foreign Service Officer, has advised that "the way out of this is to rediscover why we are an exceptional country, get to know each other better, and fight side by side."<sup>24</sup>

As all Americans are targets of the PRC's warfare,<sup>25</sup> federal agencies have responsibilities to (1) conduct outreach to citizens about the dangers they may encounter, and (2) provide appropriate incentives for Americans to proactively protect themselves—their communities, schools, houses of worship, businesses, finances, food, and more—from the threat. Federal

---

<sup>18</sup> Joske, *The party speaks for you*, *supra* note 15, at 19.

<sup>19</sup> Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World*, at 63 (2022).

<sup>20</sup> Gershaneck, *supra* note 9.

<sup>21</sup> Spalding, *War Without Rules*, *supra* note 9, at xii; *see also* Robert Spalding, *Stealth War*, at 12-13 (2019) (*Unrestricted Warfare* "should be required reading for all branches of the US government and for business leaders, because it outlines, in no uncertain terms, the strategy behind China's policies," including stating that the "new principles of war" are "no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.'").

<sup>22</sup> Gershaneck, *supra* note 9, at 16 (quoting Qiao Liang & Wang Xiangsu, *supra* note 11, at 6-7).

<sup>23</sup> Newsham, *supra* note 9, at 341.

<sup>24</sup> *Id.*

<sup>25</sup> "The Three Warfares, the traditional foundation of PRC political warfare, include public opinion/media warfare, psychological warfare, and legal warfare." Gershaneck, *supra* note 9. It "requires efforts to unify military and civilian thinking, divide the enemy into factions, weaken the enemy's combat power, and organize legal offensives." Elsa Kania, *China Brief: The PLA's Latest Strategic Thinking on the Three Warfares*, Jamestown Found. (Aug. 22, 2016).

agencies must prepare Americans to “take action.”<sup>26</sup> To stop the CCP’s “destructive actions,” retired Brig. Gen. Spalding advises that it will “take macrolevel strategic changes by our government, but also microlevel actions by individuals, businesses and other civic institutions.”<sup>27</sup> The Committee is surveying each agency’s role to secure Americans and their communities.

Congress has recognized the threat posed by the PRC for some time. Notably, in 1999, the U.S. House Select Committee on U.S. National Security and Military/Commercial Concerns with the People’s Republic of China concluded that in the preceding decade, the PRC used a “variety of techniques including espionage, controlled commercial entities, and a network of individuals that engage in contact with scientists, business people and academics” as part of its warfare operations.<sup>28</sup>

With varying degrees of effort and success, federal agencies have sought to address the CCP’s attack on what Col. Newsham has aptly described as “[t]he core of America.”<sup>29</sup> However, the threat is grave and work must be done across agencies to protect America.<sup>30</sup> Peter Mattis, former staff director of the Congressional-Executive Commission of China and counterintelligence analyst at the CIA counsels that

Only by being clear in public about the actions and intentions of the Chinese party-state, and being publicly accountable for the actions the U.S. government takes in response, will the United States be able to address Beijing’s challenges while upholding our democratic commitment to fair, transparent justice for all Americans.<sup>31</sup>

To this end, the Committee is conducting this investigation and implores each federal agency to uphold its duty to the American communities for whom they are responsible.

### CCP Disintegration Warfare Via U.S. Ports

The PRC has deployed disintegration warfare, supply chain interdiction, and cyber warfare to disrupt and capture our nation’s critical maritime and transportation networks and infrastructures.<sup>32</sup> Disintegration warfare involves “ideas of deception, disruption, and subduing

---

<sup>26</sup> Spalding, *War Without Rules*, *supra* note 9, at 214.

<sup>27</sup> *Id.*; see also Peter Mattis & Matt Schrader, *America Can’t Beat Beijing’s Tech Theft With Racial Profiling*, War on the Rocks (July 23, 2019) (“The U.S. government’s difficulties in telling a convincing story about the Chinese Communist Party point to a[n] important step: addressing a serious lack of ‘China literacy,’ both within the enforcement portions of the federal bureaucracy, and in U.S. society as a whole.”).

<sup>28</sup> Cox Report, *supra* note 9, at xxxiii; see generally Menges, *supra* note 9.

<sup>29</sup> Newsham, *supra* note 9, at 33.

<sup>30</sup> See Newsham, *supra* note 9, at 309 (“We need to know, value, protect and build the strengths of the United States of America, and shed the light of truth on the corruption, in every sense of the word,” of the CCP. “That could mean in discussions with family, community, at school or wherever that understanding needs bolstering.” Education courses on PRC political warfare would benefit “[a]ny decision-makers who work with China.”); see Gershaneck, *supra* note 9, at 153 (outlining such courses to “build[] internal defenses”).

<sup>31</sup> Mattis and Schrader, *supra* note 27.

<sup>32</sup> Liz Sly & Julia Ledur, *China has acquired a global network of strategically valuable ports*, Wash. Post (Nov. 6, 2023) (“China is now the world’s premier commercial maritime power, and its strategic hold over the world’s supply routes could be used to interdict or restrict U.S. trade, troop movements and freedom of navigation in a range of different ways. ‘It’s an asymmetrical threat.’”).

the enemy without fighting.”<sup>33</sup> Through its Belt and Road Initiative (BRI), the PRC has spent the last decade building access and influence in the open seas, strategic shipping lanes, and foreign ports around the globe.<sup>34</sup> Launched in 2013, the BRI is predicated on the weaponization of global supply chains.<sup>35</sup> It includes investments in 139 countries,<sup>36</sup> with over 100 ports in 63 countries.<sup>37</sup> When General Secretary Xi Jinping took power, he instructed top CCP leaders to turn the country into a “maritime superpower” and reminded them that “throughout history the most powerful nations were those that controlled the seas.”<sup>38</sup> Analysts have explained that BRI investments “give Beijing a window into the business dealings of competitors and could be used to help China defend its supply routes, spy on U.S. military movement and potentially engage U.S. shipping.”<sup>39</sup>

Furthermore, the BRI is linked to another CCP economic initiative known as Made in China (MIC) 2025.<sup>40</sup> Announced in 2015, MIC 2025 is “the government’s ten-year plan to update China’s manufacturing base by rapidly developing ten high-tech industries.”<sup>41</sup> The link between MIC 2025 and the BRI has been explained as follows:

BRI is aligned with China’s economic development plans, such as the 13<sup>th</sup> Five-Year Plan and the Made in China 2025 initiative. For example, BRI directly targets at least half of ten key high-technology sectors in the Made in China 2025 strategy: aerospace equipment, power equipment, new information technology, rail equipment, and marine technologies.<sup>42</sup>

What is most concerning is the fact that U.S. leaders have invited the CCP into American ports and, therefore, its critical networks and infrastructures. For example, in 2012, the Obama Administration approved a 40-year container terminal lease between the Port of Long Beach and Hong Kong-based Orient Overseas International Ltd. (OOIL), ceding control of America’s

---

<sup>33</sup> Fumio Ota, *Sun Tzu in Contemporary Chinese Strategy*, 2 J. Force Q. 76, 78 (Apr. 1, 2014).

<sup>34</sup> Elaine Dezenski & David Rader, *How China Uses Shipping for Surveillance and Control*, Foreign Pol’y (Sept. 20, 2023).

<sup>35</sup> Gerard M. Acosta, *China’s One Road One Belt Grand Strategy: Founded on the Weaponization of the Global Supply Chain*, NDTA (Dec. 1, 2020) (“China’s investment in significant global points of transportation nodes, including ports, canals, rail systems, and storage, has established the foundation to control global commercial lines of distribution a key strategic tactic to gain control of the global market.”).

<sup>36</sup> Jacob J. Lew, et al., *China’s Belt and Road: Implications for the United States*, Council on Foreign Rel. (Mar. 2021).

<sup>37</sup> John Xie, *China’s Global Network of Shipping Ports Reveal Beijing’s Strategy*, Voice of America (Sep. 13, 2021); James McBride et al., *China’s Massive Belt and Road Initiative*, Council on Foreign Rel. (Feb. 2, 2023).

<sup>38</sup> Michael Roberts, *A U.S. ‘Ships Act’ Would Break China’s Control of the Seas*, N.Y. Times (Oct. 3, 2022).

<sup>39</sup> Sly & Ledur, *supra* note 32.

<sup>40</sup> *China’s Belt and Road Initiative: Hearing Before Subcomm. on Int’l Trade, Customs, and Glob. Competitiveness of the Sen. Comm. on Fin.*, 116th Cong., at 31 (June 12, 2019) (written testimony of Carolyn Bartholomew, Chairman, U.S.-China Econ. & Sec. Rev. Comm’n) (“Bartholomew Testimony”).

<sup>41</sup> James McBride & Andrew Chatzky, *Is ‘Made in China 2025’ a Threat to Global Trade?*, Council on Foreign Rel. (May 13, 2019).

<sup>42</sup> Bartholomew Testimony, *supra* note 40, at 31.

second largest container port to the CCP.<sup>43</sup> In 2017, when Chinese state-owned shipping giant, COSCO Shipping Holdings (COSCO),<sup>44</sup> announced its intent to purchase OOIL, the Trump Administration intervened, in an attempt to remove the CCP from the Port of Long Beach. Following a national security review, the Department of Justice and Department of Homeland Security forced the newly acquired COSCO subsidiary OOIL to sell its Long Beach container terminal business,<sup>45</sup> “so COSCO would not acquire more [U.S.] infrastructure.”<sup>46</sup> However, the deal required OOIL to continue to use the Long Beach Terminal for a 20-year period.<sup>47</sup> In September 2023, the Ports of Los Angeles, Long Beach, and Shanghai announced a Green Shipping Corridor Plan intended to expedite emissions reductions.<sup>48</sup> This partnership includes PRC state-owned entities, such as COSCO.<sup>49</sup> One month later, the Ports of Los Angeles and Guangzhou “signed a Memorandum of Understanding [MOU] to further their relationship and cooperation.”<sup>50</sup> The MOU calls for collaboration on supply chains, digital technology, and “the sharing of lessons learned from the Port Optimizer, the revolutionary digital community system developed by the Port of Los Angeles and in use since 2017.”<sup>51</sup>

Furthermore, the CCP has embarked on a buying spree of U.S. ports and related critical infrastructure by hiding behind a French company. In 2013, China Merchants Group (CMG), a subsidiary of PRC state-owned China Merchants Holdings (CMH), purchased a 49 percent stake in the commercial terminal operator Terminal Link, with interests in the ports of Miami and Houston.<sup>52</sup> The other 51 percent stake is held by CMA CGM, a French company that has been

---

<sup>43</sup> See Jared Vineyard, *U.S. Forces China out of Port of Long Beach Terminal Ownership*, Universal Cargo (Oct. 15, 2019).

<sup>44</sup> “Newsweek’s reporting, and an internal COSCO publication, show how the Communist Party operates inside a company that presents itself as a modern business partner abroad but proclaims at home it ‘follows the party’s direction and sails for the motherland.’” Didi Kirsten Tatlow, *China’s Stake in World Ports Sharpens Attention on Political Influence*, Newsweek (Oct. 9, 2022).

<sup>45</sup> Costas Paris & Joanne Chiu, *U.S. Questions Cosco’s Takeover of Cargo Terminal in Long Beach*, Wall St. J. (Apr. 20, 2018).

<sup>46</sup> Tatlow, *supra* note 44.

<sup>47</sup> Enoch Yu, *US security concerns force Cosco-owned Orient Overseas to sell Long Beach port in California*, South China Morning Post (Apr. 30, 2019).

<sup>48</sup> *Ports of Los Angeles, Long Beach, Shanghai Unveil Outline For First Trans-Pacific Green Shipping Corridor*, Port of L.A. (Sept. 22, 2023) (noting that carrier partners include CMA CGM and COSCO Shipping Lines).

<sup>49</sup> *Id.*

<sup>50</sup> *Ports of Los Angeles and Guangzhou to Partner On Digital Technology and Green Shipping Corridor*, Port of L.A. (Oct. 24, 2023).

<sup>51</sup> *Id.*

<sup>52</sup> Christopher R. O’Dea, *How China Weaponized the Global Supply Chain*, Nat’l Rev. (June 20, 2019); China Merchants Group, *About Us*, (“China Merchants Holding (International) Company Ltd. and CMA CGM Group from France signed a stock purchase agreement, in which CMA CGM Group agreed to sell 49% of its wholly-owned subsidiary company Terminal Link’s stock to China Merchants Holding (International) for 400 million Euros in cash, including 15 ports overseas.”), available at <https://www.cmhk.com/en/#:~:text=China%20Merchants%20Group%20was%20founded,forward%20in%20many%20historical%20moments>, (last visited June 20, 2024); China Merchants Port Holdings Company Limited, *France* (“Terminal Link operates a network of terminals with a global reach including Far East, North Europe, Mediterranean, West Africa and North America, among them, Terminals including Malta Freeport Terminal are important hubs along the ‘One Belt and Road’ layout.”), available at <https://www.cmport.com.hk/EnTouch/business/Infor.aspx?id=10000819> (last visited June 20, 2024).

controlled by the CCP since 2015.<sup>53</sup> CMA CGM has been referred to as “a de facto French vassal line financed by Chinese state-owned lenders.”<sup>54</sup> In 2019, Secretary General Xi Jinping traveled to France to personally sign-off on a deal between the CCP and CMA CGM for 10 container megaships “from state-owned China State Shipbuilding Corp.”<sup>55</sup>

In a series of deals that have flown under the radar, the partnership between China Merchants Holdings and CMA CGM has further entrenched the CCP on American shores and empowered the Party.<sup>56</sup> In 2019, CMA CGM purchased almost 90 percent of the voting shares in CEVA Logistics AG, a company that runs the largest freight network in the U.S.<sup>57</sup> This gave control of a major U.S. logistics network “to a company that is financed by Chinese state banks and whose principal ally is the logistics arm of the Chinese navy.”<sup>58</sup> Then in 2021, CMA CGM announced its intent to acquire a majority stake in a second logistics company, “making CEVA Logistics the fourth-largest global player in contract logistics services.”<sup>59</sup> Even more concerning, in 2023, CMA CGM purchased key terminals at the Ports of New York and New Jersey.<sup>60</sup> CMA CGM described the significance of the acquisition as follows: “[t]hese two new assets provide the group with flagship terminal operations at a critical entry point on the U.S. East coast.”<sup>61</sup> Furthermore, in 2021, CMA CGM acquired the Fenix Marine Services container terminal at the Port of Los Angeles, “the third-largest container terminal at Los Angeles and its takeover will add to the 49 terminals in which CMA CGM already has investments worldwide.”<sup>62</sup>

---

<sup>53</sup> Christopher R. O’Dea, *How China Weaponized the Global Supply Chain*, *The Nat’l Review* (June 20, 2019) (explaining that “in 2015 a Chinese state bank injected more than \$1 billion into CMA CGM, in a deal that included an undisclosed strategic investment in the company and required CMA CGM to buy ships and containers from Chinese suppliers.”).

<sup>54</sup> *Id.*

<sup>55</sup> Costas Paris, *France’s CMA CGM to Buy Chinese-Made Container Ships*, *Wall St. J.* (Mar. 25, 2019).

<sup>56</sup> O’Dea, *supra* note 53 (“COSCO’s leverage is multiplied through the Ocean Alliance, one of three space-sharing arrangements that container lines formed in 2016 to help one another avoid sailing partially filled vessels. COSCO’s major ally in the Ocean Alliance is CMA CGM”).

<sup>57</sup> O’Dea, *supra* note 53; CEVA Logistics, *Responsive Logistics For You* (CEVA Logistics is a fully-owned subsidiary of the CMA CGM Group, a world leader in shipping and logistics), *available at* <https://www.cevalogistics.com/en/who-we-are/about-ceva-logistics> (last visited June 20, 2024).

<sup>58</sup> O’Dea, *supra* note 53.

<sup>59</sup> CEVA Logistics, *Breaking News* (“CEVA Logistics, a subsidiary of CMA CGM Groups, has completed the acquisition of Ingram Micro Commerce & Lifecycle Services.”) (Mar. 23, 2023).

<sup>60</sup> *CMA CGM completes the acquisition of GCT Bayonne and New York container terminals*, *CMA CGM* (Aug. 31, 2023); *France’s CMA CGM to buy New York, New Jersey terminals from Canada’s GCT*, *Reuters* (Dec. 7, 2022) (“CMA CGM said [the] acquired ports in Staten Island, New York, and Bayonne, New Jersey, have a combined capacity of 2 million twenty-foot-equivalent units per year, and has a potential for further expansion, up to almost double capacity.”).

<sup>61</sup> *CMA CGM, supra* note 60 (explaining that CMA CGM intends to further develop the two terminals, with plans to create additional yard and berth capacity, improve direct rail and road access).

<sup>62</sup> *Shipping group CMA CGM to buy Los Angeles’ FMS container terminal*, *Reuters* (Nov. 3, 2021) (“CMA CGM currently has a 10% stake in FMS and it is to buy the remaining 90%” and “[the] Los Angeles port handles massive freight volumes between China and the United States”).

Due to the serious threat posed by the CCP to our nation's critical maritime and transportation networks and infrastructures, these alliances, deals, MOUs, and similar relationships are cause for concern and warrant aggressive scrutiny by DOT and other federal agencies.

### PRC Supply Chain Interdiction and Market Dominance

In a disastrous twist of fate, America has enabled CCP state-owned enterprises to dominate the shipping container industry, giving the Party direct access to the nation's critical networks and infrastructures.<sup>63</sup> It has been reported that through the offshoring of Western manufacturing to China, the PRC has weaponized the shipping container “to reverse engineer the historical logic of international power and conquest.”<sup>64</sup> PRC state-owned companies, including CMG and COSCO, both shareholders of major Chinese shipping container producer China International Marine Containers (Group) Ltd. (CIMC), “manufacture over 95% of containers in the world's market, including U.S. domestic train and truck intermodal containers.”<sup>65</sup> It is alarming that PRC state-owned entities are also the *sole* manufacturers of the 53-foot containers used by U.S. domestic intermodal rail and trucking companies.<sup>66</sup> These intermodal containers are highly sought after by the American freight industry. For example, in 2022, a major U.S. freight forwarding company purchased 300 PRC-manufactured 53-foot containers and chartered three vessels to bring them directly from the PRC to the California Port of Hueneme.<sup>67</sup>

Even worse, these same PRC-state-owned companies reportedly “build, install, finance, and operate an integrated system connecting any economy to the world's [global] logistics network.”<sup>68</sup> It has been written that “the U.S. and China are engaged in a direct battle over the world's economic life force: technology.”<sup>69</sup> Former Treasury Secretary Henry Paulson stated “[t]he battle is about whose economy will drive the technology of the future and set the standards

---

<sup>63</sup> Fed. Highway Admin., U.S. Dept of Transp., *Freight Economy* (“Our freight transportation network is one of the great strengths of our country. Millions of Americans wake up in the morning to go to work operating trucks, trains, aircraft, ships, and barges. The system moves 55 million tons of goods worth more than \$49 billion each day. In addition, freight supports 44 million jobs. It is a critical force in our economy made up of a vast, complex network of almost seven million miles of highways, local roads, railways, navigable waterways, and pipelines.”), *available at* <https://www.fhwa.dot.gov/freighteconomy/> (last visited June 20, 2024).

<sup>64</sup> Mercy A. Kuo, *Shipping, Ports, and China's New Maritime Empire*, *The Diplomat* (Feb. 6, 2024).

<sup>65</sup> Fed. Mar. Comm'n, *Assessment of P.R.C. Control of Container and Intermodal Chassis Manufacturing Final Report*, at 3 (“The fact that the PRC controls an industry that has a near defacto worldwide monopoly in the production of shipping containers should be deeply concerning.”).

<sup>66</sup> *Id.* at 9.

<sup>67</sup> Eric Kulisch, *FedEx Logistics charters vessels to move China exports, rail containers*, *FreightWaves* (Jan. 14, 2022) (“FedEx Logistics is renting dedicated vessels so it can transport 53-foot containers manufactured in China that will be injected into the FedEx Freight intermodal network in Southern California”); Press Release, Port of Hueneme & FedEx Logistics, FedEx and Port of Hueneme Find Innovative Solutions to Supply Chain Congestion Chartering Vessels from Asia (Jan. 13, 2022).

<sup>68</sup> Kuo, *supra* note 64 (“In strategic terms, China's SOEs, primarily COSCO Shipping Group, China Merchants Port Holdings Company Ltd. and Shanghai International Port (Group) Co., Ltd., are modern versions of the Dutch East India Company”).

<sup>69</sup> Geoff Colvin, *It's China's World*, *Fortune* (July 22, 2019).



for it.”<sup>70</sup> The battle has also been described as one that “involves life-and-death issues of national security.”<sup>71</sup> An authority on the security implications of infrastructure finance and governance has explained that:

China’s economic leverage rests on one major capability that other countries lack: Logistics. Little noticed as China became the world’s manufacturing base. Chinese state-owned companies simultaneously built a global network of ports, shipping routes, container handling terminals, and transportation facilities, orchestrated by digital communications, security, and logistics software run on Chinese-operated networks.<sup>72</sup>

CCP ownership and/or operation of our nation’s ports presents serious concerns. A Foreign Policy article warns that “[f]irst, China has introduced massive and little-understood information-gathering infrastructure at critical ports worldwide. Second, Chinese laws require that all Chinese companies operating overseas—both private and state-owned—must gather and report intelligence on foreign entities to the Chinese government.”<sup>73</sup> Further, a December 2020 Department of Homeland Security advisory warned that “[t]hese laws may be used to compel PRC firms to illicitly provide the PRC government with data, logical access, encryption keys, and other vital technical information.”<sup>74</sup>

#### CCP Cyber Warfare Via Critical Networks and Infrastructures

The PRC’s global maritime operations are known to double as intelligence-gathering outposts.<sup>75</sup> In February 2024, the U.S. Maritime Administration (MARAD) issued an advisory to alert maritime stakeholders “of potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure” posed by three PRC companies.<sup>76</sup> One of those companies is the National Transportation and Logistic Public Information Platform (LOGINK), a PRC state-owned and led integrated platform for the transmission of data, which advances and expands the goals of the BRI and the Digital Silk Road.<sup>77</sup> A 2021 news report warned that “LOGINK’s international reach highlights a field critical to the world economy where the West

---

<sup>70</sup> *Id.*

<sup>71</sup> *Id.*

<sup>72</sup> Christopher R. O’Dea, *Pandemic Impact on China’s Global Expansion: Delayed, but not Derailed*, Hoover Inst. (Dec. 9, 2020).

<sup>73</sup> Dezenski & Radar, *supra* note 34.

<sup>74</sup> *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People’s Republic of China*, Dep’t of Homeland Sec. (Dec. 22, 2020).

<sup>75</sup> Dezenski & Radar, *supra* note 34.

<sup>76</sup> Mar. Admin., U.S Dep’t of Transp., *MSCI Advisory 2024-002: Worldwide-Foreign Adversarial, Technological, Physical, and Cyber Influence* (alerting maritime stakeholders about the following companies: (1) National Transportation and Logistics Public Information Platform (LOGINK), developed by the PRC Ministry of Transport; (2) Nuctech Company Ltd. (Nuctech), a PRC State-controlled entity; and (3) Shanghai Zhenhua Heavy Industries Co. (ZPMC), a subsidiary of China Communications Construction Company).

<sup>77</sup> U.S.-China Econ. & Sec. Rev. Comm’n, *LOGINK: Risks from China’s Promotion of a Global Logistics Management Platform*, at 7 (Sept. 20, 2022) (“USCC LOGINK”) (“BRI has now expanded to include economic corridors or passages on all continents. The Digital Silk Road is one such corridor, but rather than a specific geographic focus, it aims to foster export markets for Chinese tech firms and increase adoption of Chinese technical standards and governance norms globally.”).

lags behind China.”<sup>78</sup> The U.S.-China Economic and Security Review Commission concluded that “LOGINK’s visibility into global shipping and supply chains could also enable the Chinese government to identify U.S. supply chain vulnerabilities and to track shipments of U.S. military cargo on commercial freight.”<sup>79</sup> The Select Committee on the Chinese Communist Party revealed that LOGINK recently became a member of the International Port Community Systems Association (IPCSA), which “plays a role in global trade facilitation across every region of the world.”<sup>80</sup> Even more alarming, the Port of Los Angeles invited LOGINK onto American shores in 2017 through its membership in the IPCSA.<sup>81</sup>

A recent Congressional investigation into ubiquitous Chinese-built cargo cranes installed at ports throughout the U.S., including several used by the U.S. military, has uncovered that the communications equipment installed in the cranes poses a national security risk and may be used to spy on America.<sup>82</sup> These giant cranes, built by the CCP-owned company Shanghai Zhenhua Heavy Industries Co. (ZPMC), supply almost 80 percent of ship-to-shore cranes in use at U.S. ports.<sup>83</sup> DOT has explained the vital role of container cranes as follows: “[c]ontainer cranes are the critical link between the waterside and the landside, including truck and rail connections and container yards used for short-term storage.”<sup>84</sup> The Carnegie Endowment for International Peace has cautioned that “[i]f the [ZMPC] cranes were to malfunction or cease to operate normally, they could cripple U.S. transportation capacity, creating dangerous shortages and cascading

---

<sup>78</sup> Daniel Michaels, *China’s Growing Access to Global Shipping Data Worries U.S.*, Wall St. J. (Dec. 20, 2021).

<sup>79</sup> USCC *LOGINK*, *supra* note 77, at 3.

<sup>80</sup> Rep. Michelle Steel, *Defense authorization bill takes important steps to fight China’s growing influence*, The Hill (July 25, 2023); *NDAA FY 2024*, H. Sel. Comm. on the Chinese Communist Party (Dec. 14, 2023) (noting that the FY 2024 National Defense Authorization Act contains provisions to “counter[] the threat posed by CCP’s LOGINK logistics management platform at home and abroad.”).

<sup>81</sup> *Members – Europe and North America*, Int’l Port Cmty. Sys. Ass’n, available at <https://ipcsa.international/about/members/> (last visited May 14, 2024); *LOGINK signs up to IPCSA’s Network of Trusted Networks*, Int’l Port Cmty. Sys. Ass’n (Apr. 11, 2022) (“LOGINK has been a member of IPCSA since 2019 and the two organizations have had a close working relationship dating back to 2017.”); Gabriel Collins & Jack Bianchi, *China’s LOGINK Logistics Platform and Its Strategic Potential for Economic, Political, and Military Power Projection*, Baker Inst. (Apr. 25, 2023) (“Port community systems offer a critical entry point because once LOGINK is plugged into their data streams, PRC firms will not even necessarily need a physical presence at a given point in the supply chain to achieve significant data visibility and insights into cargo flows.”); USCC *LOGINK*, *supra* note 77, at 9 (Sept. 20, 2022) (describing the Network of Trusted Networks (NoTN) as: “a proof-of-concept project that will link some 70 ports and 10 airports, allowing them to share vessel and container status,” and “[membership in NoTN] could more than double LOGINK’s cooperation with global ports.”).

<sup>82</sup> Dustin Volz, *Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports*, Wall St. J. (Mar. 7, 2024).

<sup>83</sup> Press Release, H. Comm. on Homeland Sec., *WTAS: Joint Investigation Into CCP-Backed Company Supplying Cranes to U.S. Ports Reveals Shocking Findings* (Mar. 12, 2024).

<sup>84</sup> Bureau of Transp. Stat., U.S. Dep’t of Transp., *Annual Report 2024: Port Performance Freight Statistics*, at 28 (2024).

supply chain failures.”<sup>85</sup> It is no surprise that in 2021, the FBI discovered intelligence-gathering equipment on board a Chinese ship that was transporting cranes to the Port of Baltimore.<sup>86</sup>

Given Director Wray’s dire warning that “Chinese hackers are developing the ‘ability to physically wreak havoc on our critical infrastructure at a time of its choosing,’”<sup>87</sup> DOT must switch gears from reactive to proactive to protect our nation’s supply chains and national security interests. This is especially important given the fragmented nature of our nation’s transportation sector.<sup>88</sup>

### PRC Disintegration Warfare Via U.S. Rail

The CCP has weaponized its state-owned industries to devastate foreign competitors. A deleted tweet from China Railway Rolling Stock Corporation (CRRC) Limited, a CCP state-owned company, reads: “[s]o far, 83% of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take us for conquering the remaining 17%?”<sup>89</sup> This exact scenario played out in Australia where CRRC entered the freight market in 2008 and decimated domestic competition in less than ten years, leaving CRRC as the sole supplier.<sup>90</sup> In a bipartisan letter to Treasury Secretary Janet Yellen, Members of Congress warned that “CRRC’s activities in Australia should serve as a blueprint of its designs for the American market.”<sup>91</sup> This is especially concerning since the Department of Defense has identified CRRC as a national security threat with direct ties to the CCP.<sup>92</sup>

CRRC has made aggressive and dangerous inroads into the U.S. rail sector. In 2015, under the guise of American job creation,<sup>93</sup> CRRC ramped up its activities in the U.S. by

---

<sup>85</sup> Isaac Kardon, *Washington Tackles a New National Security Threat: Chinese Made Cranes*, Carnegie Endowment for Int’l Peace (Feb. 28, 2024).

<sup>86</sup> Press Release, H. Sel. Comm. on the Chinese Communist Party, Gallagher, House Homeland Security Comm. Leaders Demand Answers From CCP-Backed Company Operating at U.S. Port Amid Shocking Joint Investigation Findings (Mar. 8, 2024).

<sup>87</sup> Brie Stimpson, *Chinese hackers preparing to ‘physically wreak havoc’ on US critical infrastructure*, Fox News (Apr. 19, 2024).

<sup>88</sup> Michaels, *supra* note 78 (explaining that industry efforts to adopt an alternative to LOGINK have fallen short because “[m]ost of those efforts are led by ports, private companies, and industry alliances. Many struggle to enlist participants because the logistics industry is fiercely competitive, prompting companies to jealously guard data they fear could hand rivals an edge.”).

<sup>89</sup> *Policy Brief: China’s Infrastructure Ambitions*, All. for Innovation and Infrastructure, at 6 (Oct. 2019).

<sup>90</sup> Jimmy Quinn, *Congressmen Demand Sanctions for Chinese-Military-Linked Railway Giant*, Nat’l Rev. (Oct. 18, 2022); Letter from Mike Gallagher et al., Chairman, H. Sel. Comm. on the Chinese Communist Party, to Janet L. Yellen, Sec’y, U.S. Dept. of Treasury (Oct. 13, 2022).

<sup>91</sup> *Id.*

<sup>92</sup> Press Release, U.S. Dep’t of Def., DOD Releases List of People’s Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021 (Oct. 5, 2022); U.S. Dep’t of Def., *Entities Identified as Chinese Military Companies Operating in the United States in accordance with Section 1260H of the William M. (“Mac”) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)\*\** (2024).

<sup>93</sup> Letter from Sam Graves et al., Ranking Member, H. Comm. on Transp. & Infrastructure, to Eric Soskin, Inspector Gen., U.S. Dep’t of Transp. (Sept. 21, 2022); Thomas Fitzgerald, *A first glimpse of SEPTA’s new double-decker Regional Rail cars, under construction in China*, Phil. Inquirer (July 20, 2022).

opening a facility in Springfield, Massachusetts.<sup>94</sup> Two years later, CRRC opened a second facility in Chicago, Illinois.<sup>95</sup> From 2015 through 2020, CRRC won four passenger rail projects in the U.S., in Boston, Chicago, Philadelphia, and Los Angeles,<sup>96</sup> by significantly undercutting the competition through below market bids and CCP state-backed financing.<sup>97</sup> Even worse, CRRC has followed the PRC’s BRI “debt trap diplomacy” playbook for its rail projects in the United States.<sup>98</sup> Senator Marco Rubio has described BRI as “a one-way ticket to broken power plants and collapsing infrastructure” and warned other nations that “[i]t is not too late to learn the lesson that ‘Made in China’ projects are glorified money pits at best, and serious security threats at worst.”<sup>99</sup>

CRRC railcars in the U.S. have been plagued by delays and defects at the expense of state and local governments and the American taxpayer. In 2014, the Massachusetts Bay Transit Authority (MBTA) signed a \$566 million contract with CRRC for 284 subway cars.<sup>100</sup> In 2017, the contract was expanded to \$870.5 million, before the delivery of any new cars, bringing the total order to 404 cars.<sup>101</sup> As of March, only 130 cars have been delivered and they are permeated with serious safety and design issues.<sup>102</sup> The MBTA recently amended CRRC’s contract, extending its deadline to 2027, providing additional funding, and waiving \$90 million in penalties.<sup>103</sup> In April, the Southeastern Pennsylvania Transportation Authority (SEPTA) terminated “for cause” a \$185 million contract with CRRC that had been in the works for seven years.<sup>104</sup> SEPTA officials characterized CRRC’s work as “shoddy” and reported the company repeatedly failed to meet production deadlines.<sup>105</sup> On February 24, 2023, the DOT Office of Inspector General initiated an audit of SEPTA’s compliance with the Federal Transit

---

<sup>94</sup> Press Release, CRRC, CRRC Rail Company Breaks Ground In Springfield, Declares Global Ambitions Beyond China Merger (Sept. 4, 2015).

<sup>95</sup> Press Release, Off. of the Mayor, Mayor Emanuel, CTA, CRRC Sifang America Break Ground On New CTA Railcar Manufacturing Facility in Chicago (Mar. 16, 2017).

<sup>96</sup> *Off Track: The role of China’s CRRC in the global railcar market*, Oxford Econ., at 22 (July 2022).

<sup>97</sup> *Id.*

<sup>98</sup> Michael Bennon & Francis Fukuyama, *China’s Road to Ruin The Real Toll of Beijing’s Belt and Road*, For. Aff. (Sept./Oct. 2023).

<sup>99</sup> Marco Rubio, *Made in China Infrastructure is often a glorified money pit*, Nikkei Asia (Feb. 9, 2023).

<sup>100</sup> Gayla Cawley, *Timeline of MBTA’s \$870.5M contract with Chinese-owned CRRC*, Boston Herald (Feb. 18, 2023) (writing that “[c]ritics pointed to the Chinese-state-owned company significantly underbidding its competitors and its ties to the Communist Party, with some even asserting there was the potential for spyware installation in trains.”).

<sup>101</sup> *Id.* (explaining that CRRC received an exemption from the National Defense Authorization Act for Fiscal Year 2020, “which bans mass transit agencies from using federal funds for the purchase of rail cars and buses from Chinese-owned companies.”)

<sup>102</sup> James Paleologopoulos, *MBTA updates contract with CRRC to complete railcars at Springfield plant*, WAMC Public Radio Northeast (Mar. 29, 2024).

<sup>103</sup> *Id.* (noting that officials in Los Angeles have also given CRRC production extensions.).

<sup>104</sup> Jessica MacAuley, *SEPTA hits the brakes on double-decker train cars for regional rail system*, CBS News (Apr. 14, 2024).

<sup>105</sup> Elizabeth Brotherton-Bunch, *Philadelphia’s SEPTA Transit System Officially Cancels Its Disastrous Rail Car Contract with Chinese State-owned Firm CRRC*, All. for Am. Manu. (Apr. 15, 2024).

Administration's (FTA) Buy America requirements.<sup>106</sup> Furthermore, Chicago's \$1.3 billion dollar contract with CRRC Sifang for railcars came under scrutiny for serious human rights abuses.<sup>107</sup> According to an NBC investigative report, PRC state-controlled entities in Madagascar were using children as young as two years old to mine for mica that later ended up in products sold by CRRC.<sup>108</sup>

DOT must ramp up its oversight to ensure state and local governments do not side-step federal procurement laws,<sup>109</sup> and protect public funds and American taxpayers from fraud, waste, and abuse in ways that benefit the authoritarian CCP regime.

### Conclusion

It is critical that DOT do everything in its power to counter CCP infiltration into America's maritime and transportation networks and infrastructures. The tragic collapse of the Francis Scott Key Bridge in Baltimore is a stark reminder that our roads, bridges, and ports are inextricably linked to both national and global supply chains.<sup>110</sup> At a recent press conference to discuss the collapse of the bridge, you acknowledged concerns about implications that will extend out beyond the immediate region "because of the port's role in our [nation's] supply chains."<sup>111</sup> DOT has significant work to do to address the threat of CCP economic and cyber warfare threatening our nation's critical maritime and transportation networks and infrastructures.

To assist the Committee in investigating this matter, we request a briefing from the DOT with Committee staff. Please contact Committee staff as soon as possible, but no later than June 28, 2024. This briefing should address the following:

---

<sup>106</sup> Memorandum from the Off. of Inspector Gen., U.S. Dep't of Transp., to the Fed. Transit Admin. on Audit Announcement: FTA Oversight of the Southern Eastern Pennsylvania Transportation Authority's Compliance with Buy America Requirements for Rolling Stock (Feb. 24, 2023) ("Per FTA's Buy America requirements, the cost of the components and subcomponents for rolling stock produced in the United States must total more than 60 percent for fiscal years 2016 and 2017, more than 65 percent for fiscal years 2018 and 2019 and more than 70 percent for fiscal year 2020 and beyond. In addition, final assembly of rolling stock must occur in the United States.").

<sup>107</sup> Robert Herguth, *CTA wants answers from Chinese L car manufacturer after NBC report on child labor*, Chicago Sun-Times (Dec. 5, 2019).

<sup>108</sup> Lisa Cavazuti et al., *'Zone Rouge': An army of children toils in African mines*, NBC News (Nov. 18, 2019) ([t]hese firms turn the mineral shards into component parts that end up in products sold by [] CRRC, a Chinese government-owned rail equipment manufacturer that has signed deals to produce trains for Los Angeles, Chicago, Philadelphia and Boston.").

<sup>109</sup> U.S. Gov't Accountability Off., GAO-22-88, *States and Local Governments Reported Benefits to Federal Highway Fund Swapping, but Impacts Cannot be Definitively Determined* (Oct. 2020) (GAO concluded that "the ability of local agencies to comply with federal requirements is a well-documented risk area" and "[s]ome states have established 'fund swapping' programs where local agencies swap proposed federal funding with the state in return for state dollars.").

<sup>110</sup> Ryan Petersen, *I Work in Supply Chain Logistics. Here's What I Advise After the Tragedy in Baltimore*, N.Y. Times (Mar. 27, 2024).

<sup>111</sup> *TRANSCRIPT: Press Briefing by U.S. Secretary of Transportation Pete Buttigieg, Press Secretary Karine Jean-Pierre, and Deputy Commandant for Operations for the U.S. Coast Guard Vice Admiral Peter Gautier*, U.S. Dep't of Transp. (Mar. 27, 2024).

1. How DOT strives to inspire and equip Americans to strengthen their communities, innovate, and create the technologies and phenomena that will secure a strong and prosperous future for our nation;
2. How DOT leadership ensures from the top down that all DOT employees are aware of CCP warfare and influence operations against America, and are equipped to address them wherever they arise;
3. DOT Leadership, Outreach, and Training to Defeat CCP Warfare
  - a. How DOT leadership ensures the CCP and PRC have no footprint in U.S. transportation and infrastructure, whether through ownership, equipment, surveillance, or otherwise;
  - b. DOT outreach to the American public, the transportation industry, and U.S. Ports regarding CCP economic and cyber warfare targeting U.S. infrastructure;
  - c. DOT training of employees to identify and counter CCP economic and cyber warfare threatening U.S. infrastructure;
4. Collaboration to Identify and Counter CCP Warfare
  - a. What steps DOT is taking alone or in coordination with other agencies and outside stakeholders to guard against cyber and espionage threats posed by PRC-manufactured shipping containers and intermodal containers in the U.S.;
  - b. How DOT works with state and local governments across the country to ensure they are prepared for CCP cyber warfare threats against our nation's maritime and transportation networks and infrastructures;<sup>112</sup>
  - c. How DOT is working with the Federal Maritime Commission, U.S. Customs and Border Protection and other stakeholders to develop an alternative to LOGINK that cannot be infiltrated by foreign adversaries;
  - d. How DOT engages with and ensures coordination between private stakeholders to ensure they are prepared for CCP cyber and economic warfare threats against our nation's maritime and transportation networks and infrastructures;
5. Key Maritime & Transportation Infrastructure Sectors Targeted by the CCP

---

<sup>112</sup> Christina Goldbaum et al., *The M.T.A. Is Breached by Hackers as Cyberattacks Surge*, N.Y. Times (July 20, 2021); Scott Belcher et al., *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, Mineta Transp. Inst., at 32 (Sept. 2020) (noting that only 60 percent of transportation agencies had a cybersecurity plan in place).

- a. How DOT is working to secure our nation's oil and gas pipelines from CCP cyber warfare;
  - b. How DOT is working to ensure the U.S. aviation industry and air travelers are not harmed by unfair competition from the PRC;
  - c. What steps DOT is taking to address our nation's sealift vessel shortage to make sure our nation is prepared to respond to a conflict in the Indo-Pacific;<sup>113</sup>
  - d. How DOT is working to implement PRC reciprocity<sup>114</sup> across all transportation sectors to address competition concerns regarding the PRC; and
6. Fraud, Waste and Abuse
- a. How DOT audits its grant programs at the federal, state, and local level to ensure compliance with federal regulations and policies, including to ensure taxpayer dollars are not flowing back to China or the CCP, and to protect against fraud, waste and abuse.

Please contact the Committee staff at (202) 225-5074 to schedule the staff briefing. The Committee on Oversight and Accountability is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. Thank you for your prompt attention to this important investigation.

Sincerely,



James Comer  
Chairman  
Committee on Oversight and Accountability

cc: The Honorable Jamie B. Raskin, Ranking Member  
Committee on Oversight and Accountability

---

<sup>113</sup> Letter from Mike Gallagher, Chairman, H. Sel. Comm. on the Chinese Communist Party, to Gen. Jacqueline D. Van Ovost, Commander Transp. Command, U.S. Dep't of Def., Ann C. Phillips, Admin., Mar. Admin., U.S. Dep't of Transp. (Feb. 6, 2024).

<sup>114</sup> David Ingram, *Chinese tech startups are testing self-driving cars on California roads*, NBC News (Oct. 3, 2023) (Commerce Sec'y Raimondo testified that "it was 'very clear' to her [when she visited China] that U.S. self-driving startups weren't welcome there in the way Chinese firms had been welcomed here," and that while China's "autonomous vehicle companies are piloting on our roads right now; we cannot." She testified: "Let's level the playing field.").