COALITION for a PROSPEROUS AMERICA

Phone: 202-688-5145
Email: info@prosperousamerica.org
Website: prosperousamerica.org

December 15, 2021

Laurence D. Fink
Chairman and Chief Executive Officer
BlackRock
55 East 52nd Street
New York, NY10055

Dear Mr. Fink,

We are writing to bring to your attention the serious human rights abuses and U.S. national security risks associated with certain Chinese companies held in BlackRock's iShares Exchange-Traded Funds (ETFs).

Our review of the holdings (as of October 31, 2021) of the iShares ESG Aware MSCI EM ETF (ESGE), iShares Core MSCI Emerging Markets ETF (IEMG), iShares MSCI China ETF (MCHI), and iShares MSCI China A ETF (CNYA) products found that these funds are currently holding the securities of eight companies that have been placed on the U.S. Department of Commerce's Entity List for egregious human rights abuses, as well as three companies that are on the U.S. Department of the Treasury's Non-SDN Chinese Military Industrial Complex Companies (CMIC) List for their involvement in China's military and surveillance sectors. We have highlighted the risk profiles of four of these companies in the attached Appendix.

By purchasing shares in these ETFs, American retail and institutional investors are exposed to a wide range of publicly traded Chinese companies that are involved in activities that are contrary to U.S. national and economic security interests and human rights values. A number of these companies are also under U.S. economic sanctions and export controls because they pose a direct risk to U.S. national security and are facilitating the strategic agenda of the Chinese Communist Party (CCP), including the modernization of the People's Liberation Army and Navy and China's ongoing genocide against the Uyghurs and other Muslim minorities in Xinjiang.

MSCI's criteria, and those of other index providers, to evaluate companies listed in its products fails to consider material risks posed to U.S. national security, sanctions regimes, and human rights violations. These gaps in oversight and due diligence make BlackRock's iShares investment products the conduit for millions of unwitting American retail investors – including through pension funds managed by BlackRock – to fund Chinese companies that are officially recognized as actively undermining the U.S. security interests, our nation's fundamental values and American companies and workers.

The publicly traded securities issued by these Chinese firms also represent serious financial risks for U.S. investors, including their failure to comply with the Public Companies Accounting Oversight Board's (PCAOB) rules for transparency and disclosure. As BlackRock knows, China- and Hong Kong-based companies do not comply with the PCAOB's audit requirements, opening up American retail investors to serious fiduciary risk and potential fraud by these firms. The list of fraudulent Chinese firms listed publicly on U.S. exchanges continues to grow. While Congress

and independent regulators have begun to take action to address this risk, BlackRock has not publicly addressed what, if anything, it is doing to mitigate the presence of these Chinese corporate "bad actors" in its investment products.

Congress passed the *Holding Foreign Companies Accountable Act* (HFCAA) to bring China- and Hong Kong-based companies into compliance with U.S. securities laws, but this new legislation only affects Chinese companies listed directly on U.S. exchanges. It neglects to address more than 4,200 “A-Share” securities of companies that are still available to U.S. investors through passive investment products like BlackRock’s.

Both the Trump and Biden administrations have issued Executive Orders banning U.S. investment in securities of Chinese companies found to present a national security threat to the United States. Indeed, the scope of these restrictions continues to expand, with the inclusion of certain human rights abuses (e.g. surveillance technology companies) in President Biden’s Executive Order 14032 and the commitment to continue to add Chinese companies to the Non-SDN Chinese Military Industrial Complex Companies (CMIC) List, most recently on display last week with the addition of SenseTime to this latter list.

Congress and the Biden administration are also considering expanding capital markets restrictions on Chinese companies. In fact, there is a growing bipartisan consensus that the U.S. government should take action to address the issues raised above. BlackRock is well aware of this positive shift in policy and of its roots evidenced by official and non-governmental public reports over the past eighteen months linking companies included in BlackRock products to serious national security and human rights transgressions As this oversight, legislative, and regulatory trajectory continues, fund managers will inevitably be required to remove additional Chinese companies from ETF holdings, and ultimately implement far stricter due diligence procedures for Chinese securities than the near-zero diligence of today.

We strongly urge BlackRock, through its iShares business, to engage directly with MSCI and urge them to exclude Chinese companies from its indices that have public records of human rights abuses in Xinjiang and throughout the People’s Republic of China, or those Chinese firms that have been credibly identified by the U.S. government as part of China’s military-industrial complex and program of military-civil fusion.

As the CCP continues its efforts to undermine U.S. economic and national security and the public becomes more aware and outraged by this allocation of their money, there will be ever-greater scrutiny of those American asset managers and other firms that have chosen to profit off of aiding and funding the Chinese Communist Party instead of acting in the best interests of our nation and American retail investors.

Sincerely,

Zach Mottl, Chairman
Coalition for a Prosperous America

Michael Stumo, CEO
Coalition for a Prosperous America

APPENDIX I

Inspur Group Co., Ltd.
Listed Subsidiaries: Inspur Software Co., Ltd. 600756.SS, Inspur International 000977.SZ, 0596.HK

Inspur is a high-tech company that has significant connections to the Chinese government, and to Chinese military and security services. According to a report from Defense One, the People's Liberation Army (PLA) uses Inspur equipment and computers, mapping technology, and communications equipment.[1]

Inspur also famously worked from 2013-2015 with China's National University of Defense Technology to build the world's fastest supercomputer, China's Tianhe-2, on an 863 grant. The supercomputer was reportedly used for government security and military applications. The 863 Program has been accused of serving as the Chinese military's vehicle for espionage, intellectual property theft,. According to a 2011 report from the U.S. Office of the National Counterintelligence Executive, the 863 program "provides funding and guidance for efforts to clandestinely acquire U.S. technology and sensitive economic information."[2]

In April 2015, the U.S. government Department of Commerce imposed export controls on Inspur prohibiting the use of U.S. equipment and technology in Inspur's supercomputer program due to military and security concerns.[3]

China State Shipbuilding Corporation (CSSC)
Listed Subsidiary: China CSSC Holdings Ltd. 600150.SS

CSSC is involved in the Chinese government's efforts to reclaim and militarize disputed areas of the South China Sea. In May 2014, a research institute under China State Shipbuilding Corporation (CSSC) released plans on its website to build an artificial island, an airstrip complex, and a possible military base at the Johnson South Reef.[4]

In December 2015, CSSC announced that it would begin building an underwater observation system coined the "Underwater Great Wall" in the South China Sea, under a contract with the PLA. The massive underwater surveillance system will feature a network of ship and underwater subsurface sensors, providing the PLA Navy with a significant tactical advantage in the disputed and increasingly tense South China Sea. [5]

---

[1] https://www.nytimes.com/interactive/2015/10/30/technology/US-Tech-Firms-and-Their-Chinese-Partnerships.html?mtrref=www.google.com&assetType=REGIWALL

[2] https://www.wsj.com/articles/nsa-concerns-give-chinese-server-maker-inspur-a-boost-1406653858

[3] https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

[4] https://www.popsci.com/chinese-shipyard-looks-build-giant-floating-islands/

[5] https://www.popsci.com/chinese-shipyard-looks-build-giant-floating-islands/

CSSC was included he Executive Order issued in November 2020 that prohibited U.S. investors from owning shares in companies linked to the PLA by the U.S. DOD. CSSC was included in this list.[6]

Zhejiang Dahua Technology Co., Ltd. 002236.SZ
Dahua Technology provides video surveillance products and services used in machine vision, video conferencing, professional drones, and RFID systems. It has received over a billion dollars in contracts for video surveillance and security projects in Xinjiang, including facial recognition and data storage systems.[7]
The company was added to the U.S. Department of Commerce's Entity List in October 2019 for having been implicated in human rights violations and abuses, mass arbitrary detention, and high-tech surveillance in Xinjiang. Dahua Technology was also one of the five Chinese companies that was designated as a national security threat by the Federal Communications Commission (FCC) in March 2021.[8]
iFlytek 002230.SZ

Iflytek produces speech recognition software and products, including the first AI open platform for smart hardware developers in China. It has supplied voiceprint collection systems to Kashgar police in Xinjiang and partnered with the Xinjiang Public Security Bureau and with telecommunications companies to integrate voice pattern data into surveillance systems.[9]

Iflytek was added to the U.S. Department of Commerce's Entity List in October 2019 for having been implicated in human rights violations and abuses, mass arbitrary detention, and high-tech surveillance in Xinjiang.[10]

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/

[7] http://www.its114.com/html/2017/changshangyaowen_0217/84407.html; https://ipvm.com/reports/xinjiang-dahua-hikvision

[8] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

[9] https://www.reuters.com/article/us-china-xinjiang-mit-tech-insight/risky-partner-top-u-s-universities-took-funds-from-chinese-firm-tied-to-xinjiang-security-idUSKCN1TE04M; https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

[10] https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list