March 29, 2021

ALLIANCE FOR american manufacturing

Steve Poftak
MBTA General Manager and Chief Executive Officer
MBTA's Material Management Office
10 Park Plaza, Suite 2810
Boston, MA 02116

Dear Mr. Poftak:

On behalf of the Alliance for American Manufacturing, I write in regard to the MBTA's announced commuter rail fiber optic network resiliency project to remind the Authority that Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits federal grant recipients from procuring or contracting certain telecommunications equipment, systems, or services from the People's Republic of China. Congress and a number of national security experts have determined that these entities – which includes Huawei – pose a host of threats to the United States.[1] In light of its current contract with China Railway Rolling Stock Corporation (CRRC) – the Chinese state-owned rail rolling stock manufacturer with documented partnerships with Huawei – and its solicitation of letters of interest for the commuter rail fiber optic network resiliency project, the MBTA is reminded of the Sec. 889 prohibitions and strongly encouraged to conduct this procurement in a manner that is fully compliant with this federal law.

The 2019 report, "CRRC and Beijing's Dash for Global Rolling Stock Dominance," documents CRRC's various partnerships with Chinese telecommunications entities, including those that are restricted by Sec. 889, as well as China's Communist Party and the People's Liberation Army. [2] Based on these security threats and the funding prohibition contained in Sec. 889, MBTA should immediately disqualify any covered telecommunications equipment or services. In fact, it is notable that CRRC partners with now-banned Huawei – as well as BeiDou, a Chinese satellite navigation system – in building technologies and information systems that threaten individual and data security.

Report excerpts:

- CRRC also works with other entities that the United States has already labeled as predatory actors or national security threats. For example, CRRC actively cooperates with Huawei, connecting the physical infrastructure of rail to Huawei's information technology networks in pursuit of a government-linked "Internet of Things with Chinese characteristics."[3]

- China's Ministry of Industry and Information Technology (MIIT) and the National Standardization Administration run a "two in one integration management platform," a "strategic deployment of the Party Central Committee" designed to collect and to integrate information across the industrial system and to use that to claim related standards – to create a large-scale industrial internet, under the Chinese government, radiating internationally. CRRC is not just a member of the platform. It is also on the Guiding Committee, alongside China Ordnance Equipment Group, MIIT's Electronics

[1] Section 889 of the FY19 National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019), Pub. L. No. 115-232 (Aug. 13, 2018)
[2] "CRRC and Beijing's Dash for Global Rolling Stock Dominance," Bruyere and Picarsic. Radarlock. October 2019.
[3] Ibid at 17

Institute, the State Grid Corporation, China Mobile, Huawei, Tsinghua, Beijing Aerospace University, Haier, and ZTE, among others.[4]

- In May 2018, CRRC subsidiary CRRC Zhuzhou joined with Huawei to develop a light rail system.[5]

- In March 2019, Jiangsu CRRC Digital Technology Co., Ltd, another CRRC subsidiary, and Huawei signed a "strategic cooperation agreement" where '[t]he two parties will partner extensively in the fields of industrial Internet platform construction and intelligent manufacturing." [6]

- Chinese reporting on the agreement notes that the firms will focus on "developing the strategy of China CRRC Group in transforming, upgrading, and transnational operations; the two sides will jointly promote the construction and application of the industrial Internet platform, build a 'digital car' project, and realize the digitization and digital industry of CRRC." [7]

- "The strategic cooperation agreement will rely on Huawei's strong R&D and strength in big data cloud computing and information and communications technology." Discussion of the cooperation stresses that CRRC digital products appear across "aerospace, aviation, rail transit, machinery manufacturing, military, and other fields." The clear implication is that the Huawei and CRRC cooperative network will extend also to those domains. [8]

- Cooperation involves partnership on a 5G system – with it, monitoring and data sharing. Huawei and CRRC's Zhuzhou subsidiary jointly developed a "5G system" in Chengdu.[9]

- The month after the announcement of the strategic cooperation agreement between CRRC and Huawei, the latter's investment arm, Hubble Technology, invested in two semiconductor- related companies. One of them was Shandong Tianhua, whose core silicon carbide material product is a focus of Made in China 2025. That company's founder acknowledged in 2014 that it was "under the leadership of relevant State ministries and commissions as well as key enterprises of the industrial chain," including China South Rail [the company that would become CRRC], and Huawei Hisilicon."[10]

- Beidou – China's space champion and one of its top Military Civil Fusion MCF instruments – offers another prime example of the concerns. In February 2016, CRRC's subsidiary Dalian Electric Co. signed a "strategic cooperation framework agreement" with Beidou. [11]

[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid at 18

March 29, 2021

ALLIANCE FOR american manufacturing

As the U.S.-China Economic & Security Review Commission has noted, "some private Chinese companies operating in strategic sectors are private only in name, with the Chinese government using an array of measures, including financial support and other incentives, as well as coercion, to influence private business decisions and achieve state goals."[12] This fiber optic system, supporting one of the largest subway systems in the world is an important component of our critical infrastructure. As we learned as part of the 9/11 attacks on New York, the resiliency and integrity of our telecommunications network is not only key to those at risk during a potential event, but also a key component of a system to manage and reduce public distress. Relying on a company that, under China's national security laws must abide by the Chinese Communist Party's orders is unacceptable.

Moreover, Americans of all political backgrounds believe that their tax dollars should be spent on U.S.-made products. American workers stand ready to supply the materials needed, and there are more than 750 companies in at least 39 states manufacturing components for transit and passenger rail. At a time when COVID-19 related economic fallout has cost tens of millions of Americans their jobs, including hundreds of thousands of manufacturing workers, we strongly urge you to focus your procurement efforts on secure, domestic sources rather than on shortsighted partnerships with Chinese state-owned enterprises and entities that pose a threat to U.S. security interests.

Sincerely,

Scott N. Paul, President
Alliance for American Manufacturing

cc: Jamey Tesler, Mass DOT Acting Secretary and Chief Executive Officer

[12] US-China Economic and Security Review Commission, 2017 Annual Report to Congress, at 3.