OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
16 DECEMBER 2020 IA-48113-21

ECONOMIC SECURITY

(U//FOUO) Chinese Television Manufacturer Likely Poses Security Risk

(U//FOUO) ***We assess that the People's Republic of China (PRC) likely has influence over the TCL Technology Group Corporation (TCL), a prominent Chinese electronics firm.*** We base this assessment on the roles that key TCL leaders have served in the Chinese Government and assessed state-owned entities (SOEs), as well as on financial support provided by the PRC to TCL. TCL is the third-largest global television manufacturer by sales, producing more than 28 million units worldwide, according to a US international affairs magazine.

- *(U//FOUO)* Li Dongsheng, who founded TCL and serves as its Chairman and Executive Director, served in at least five iterations of the PRC's National People's Congress since 2002, according to an open-source Chinese biographical database and information from a US financial firm. Dongsheng is also the Chairman of the China Chamber of International Commerce and Vice Chairman of the China Federation of Industry and Commerce, both of which are state-run entities, according to information from a US financial firm, the organizations' websites, and a Chinese news outlet.
- *(U)* Yang Zhe, who serves as the President and Chief Operating Officer of TCL Communications Technology Holdings, a subsidiary of TCL, previously served as Chief Management Officer of Huawei Technologies from 2012 through 2015, according to information from a US financial company. Huawei is assessed to be a Chinese SOE and has been included on the Department of Commerce's Entity List, according to a press report.
- *(U)* TCL is able to undercut competitors because of financial assistance provided by the PRC, such as $74.5 million in subsidies from the Chinese city of Shenzhen in 2010, according to a US international affairs magazine.

(U//FOUO) ***TCL likely has the ability to collect data from the US Government and other consumers because of its ability to incorporate components with embedded design vulnerabilities.*** The company maintains a vertically integrated manufacturing process, producing every component that goes into each TCL television.

- *(U)* According to a US-based security blog, TCL has incorporated a backdoor into all of its TV sets, which can be accessed remotely without the owner's permission or awareness. The backdoor enables an attacker to download system files from the TV that can include personal data, images, and tokens for connected applications, according to the same source.

(U) Prepared by the Economic Security Mission Center. Coordinated within the DHS Intelligence Enterprise (CIMC, CWMD, ICE, USCG, HSI) and with the Current and Emerging Threats Center. For questions, contact DHS-SPS-RFI@hq.dhs.gov.

(U//FOUO) ***Should TCL acquire or partner with US electronics companies, we assess that the company would pose a risk to US intellectual property.*** The PRC often uses joint venture and licensing agreements, in addition to foreign direct and venture capital investments, to acquire US intellectual property, according to research by a US think tank.

- *(U)* In 2017, the Swedish mobile phone manufacturer Ericsson accused TCL of obtaining a license for Ericsson's 2G patent technology and then using Ericsson's 3G and 4G/LTE technology without proper licensing, eventually selling 250 million phones with the stolen technology, according to a court document. TCL subsequently settled the patent infringement suit for $75 million, according to two legal news source.

Source, Reference, and Dissemination Information

Source Summary Statement	*(U)* This *Intelligence In Focus* is based on a collection of open-source reporting from proprietary financial databases and foreign and US news outlets. *(U//FOUO)* We assess that the PRC likely has influence over TCL. We have **moderate confidence** in this judgment based on multiple corroborative and credible sources from a US financial firm, a Chinese biography database, two China-based websites, and a US international affairs magazine. *(U//FOUO)* We assess that TCL likely has the ability to collect data from the US Government and other consumers because of its ability to incorporate components with embedded design vulnerabilities. We have **moderate confidence** in this judgment based on reporting from a credible security blog. *(U//FOUO)* Should TCL acquire or partner with US electronics companies, we assess that the company would pose a risk to US intellectual property. We have **moderate confidence** in this judgment based on documents from the US Supreme Court, a legal blog, and a US-based think tank.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and private sector security partners
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) Chinese Television Manufacturer Likely Poses Security Risk

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Drive planning and preparedness efforts, training, and/or emergency response operations
- ☐ Observe, identify, and/or disrupt threats
- ☐ Share with partners
- ☐ Allocate resources (e.g. equipment and personnel)
- ☐ Reprioritize organizational focus
- ☐ Author or adjust policies and guidelines
- ☐ Initiate a law enforcement investigation
- ☐ Intiate your own regional-specific analysis
- ☐ Intiate your own topic-specific analysis
- ☐ Develop long-term homeland security strategies
- ☐ Do not plan to use
- ☐ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:		*Position:*	
Organization:		*State:*	
Contact Number:		*Email:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**