

2017-2021 ARCHIVED CONTENT

You are viewing ARCHIVED CONTENT released online from January 20, 2017 to January 20, 2021.

Content in this archive site is NOT UPDATED, and links may not function.

For current information, go to www.state.gov.

★ ★ ★

The Clean Network Safeguards America's Assets

FACT SHEET

OFFICE OF THE SPOKESPERSON

AUGUST 11, 2020

Share 

"The spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States."

—President Donald J. Trump, August 6, 2020

"We've urged countries to become Clean Countries so that their citizens' private information doesn't end up in the hand of the Chinese Communist Party."

—Secretary of State Michael R. Pompeo, July 23, 2020

Just as the Trump Administration has taken unprecedented action to defend our physical

borders, it is also defending the United States on cyber frontiers.

- ◆ On April 29, 2020, Secretary Pompeo announced that, as part of the 2019 National Defense Authorization Act, the State Department will require a Clean Path for all standalone 5G network traffic entering and exiting U.S. diplomatic facilities at home and abroad.
- ◆ On August 5, 2020, Secretary Pompeo announced the expansion of The Clean Network to include Clean Carrier, Clean Store, Clean Apps, Clean Cloud, and Clean Cable.
- ◆ On August 6, 2020, President Trump signed two Executive Orders exercising his authority under the International Emergency Economic Powers Act (IEEPA) to address the threats posed by apps such as TikTok and WeChat.

The Clean Network Lines of Effort

The Clean Network initiative is a comprehensive effort to address the long-term threat to data privacy, security, and human rights posed to the free world from authoritarian malign actors, such as the Chinese Communist Party (CCP). The Clean Network is rooted in internationally accepted digital trust standards and is a reflection of our commitment to an open, interoperable, and secure global internet based on shared democratic values and respect for human rights. This effort represents the execution of a multi-year, all-of-government enduring strategy, built on a coalition of trusted partners.

- ◆ **5G Clean Path:** To protect the voice and data traversing 5G standalone networks entering and exiting U.S. diplomatic facilities at home and abroad. Announced by Secretary Pompeo on April 29, 2020, the 5G Clean Path is an end-to-end communication path that does not use any transmission, control, computing, or storage equipment from untrusted IT vendors, such as Huawei and ZTE, which are required by Chinese law to comply with directives of the CCP. The 5G Clean Path embodies the highest standards of security against untrusted, high-risk vendors' ability to disrupt, manipulate or deny services to private citizens, financial institutions, or critical infrastructure. All mobile data traffic entering American diplomatic systems will be subject to new, stringent requirements.
- ◆ **Clean Carrier:** To ensure untrusted People's Republic of China (PRC) carriers are not connected with U.S. telecommunications networks. Such companies pose a danger to U.S. national security and should not provide international telecommunications services to and from the United States.
- ◆ **Clean Store:** To remove untrusted applications from U.S. mobile app stores. PRC apps

threaten our privacy, proliferate viruses, censor content, and spread propaganda and disinformation. On August 6, 2020, President Trump signed two Executive Orders to address the threats posed by TikTok and WeChat. TikTok and WeChat capture vast swathes of data from their unsuspecting users and are compelled by Chinese law to turn over this private information to the CCP upon request. The American people's most sensitive personal and business information must be protected on their mobile phones from exploitation and theft for the CCP's benefit.

- ◆ **Clean Apps:** To prevent untrusted PRC smartphone manufacturers from pre-installing—or otherwise making available for download—trusted apps on their apps store. Huawei, an arm of the PRC surveillance state is trading on the innovations and reputations of leading U.S. and foreign companies. These companies should remove their apps from Huawei's app store to ensure they are not partnering with a human rights abuser.
- ◆ **Clean Cloud:** To prevent U.S. citizens' most sensitive personal information and our businesses' most valuable intellectual property, including COVID-19 vaccine research, from being stored and processed on cloud-based systems built or operated by untrusted vendors, such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent.
- ◆ **Clean Cable:** To ensure the undersea cables connecting our country to the global internet are not subverted for intelligence gathering by the PRC at hyper scale. We will also work with foreign partners to ensure that undersea cables around the world aren't built or operated by untrusted vendors.

Clean Countries and Territories

The United States is joined in The Clean Network by more than thirty like-minded Clean Countries and Territories who have committed protecting their 5G networks from untrusted vendors and/or their telecommunications carriers have agreed to only use trusted vendors. Examples include:

Albania

Australia

Canada

Czech Republic

Denmark

Estonia

France

Greece

Israel

Japan
 Latvia
 Norway
 Poland
 Romania
 Slovenia
 Sweden
 Taiwan
 United Kingdom
 USA
 Vietnam

Notable quotes:

- ◆ Prime Minister of Poland Mateusz Morawiecki stated: “Poland believes the construction of our 5G Clean Path network is a prerequisite for EU strategic technological sovereignty. That is why we must keep it secure at all costs and we are a 5G Clean Country. To protect our 5G network from potential wrongdoers it is necessary that all European entrepreneurs maintain clean production lines and a 5G Clean Path, free from potential industrial espionage. Demanding that 5G Clean Standards are observed with regard to 5G technology is a step towards building a fairer globalized world.”
- ◆ European Commissioner Thierry Breton remarked on the clean EU 5G toolbox: “The European Union with all member states developed a 5G cybersecurity toolbox defining the criteria and clear measures to avoid the use of ‘high-risk suppliers.’ The toolbox adds that member states have identified certain non-EU countries with state-backed actors as a serious cyber threat to their national interest. The European 5G suppliers are likely to meet these criteria. It will serve as a reference for the telco operators’ board of directors who have to make the decision on 5G suppliers. If they choose a ‘high-risk 5G supplier,’ the board members may be liable if something happens.”

Clean Telcos

Many of the largest telecommunications companies around the globe are becoming Clean Telcos by choosing to only use trusted vendors for their 5G network buildouts. Orange in France, Jio in India, Telstra in Australia, SK and KT in South Korea, NTT in Japan, Hrvatski Telekom in Croatia, Tele2 in Estonia, Three in Ireland, LMT in Latvia, Vodafone Ziggo

In the Netherlands, Plus in Poland, Singtel in Singapore, TDC in Denmark, O₂ in the United Kingdom, and all the 5G telcos in Canada, Norway, Vietnam, and Taiwan are rejecting doing business with tools of the CCP's surveillance state, like Huawei.

Notable quotes:

- ◆ Telefónica states in its Digital Manifesto that “security is paramount,” and its CEO and Chairman José María Álvarez-Pallete López declared, “Telefónica is proud to be a 5G Clean Path company. Telefónica Spain and O₂ (UK) are fully clean networks, and Telefónica Deutschland (Germany) and Vivo (Brazil) will be in the near future without equipment from any untrusted vendors.”
- ◆ CEO Jun Sawada of Japan’s NTT: “The safety and security of our customers and their personal information is our top priority. In this context, the statement by U.S. government regarding 5G Clean Network is consistent with our position. That is why we are glad to be appreciated as a 5G Clean Telecommunications company and are committed to only using trusted vendors in our 5G networks in Japan and as we expand our business around the world.”
- ◆ Telekom Albania CEO Emil Georgakiev: “5G networks will play a critical role in the lives of individuals and business, with any malfunction of infrastructure or leakage of data having a devastating impact on society. That’s why Telekom Albania continues to show its commitment to the highest standards of network security for our customers and our partners by using only trusted equipment. We are proud to be a 5G Clean Path partner.”
- ◆ Oracle CEO Safra Catz: “Oracle shares the vision of secure, trusted and resilient 5G applications and networks. Grounded in our commitment to develop the most secure telecommunications and infrastructure products and services for our customers, we are proud to support the Clean Path initiative and provide Clean Path solutions.”
- ◆ VMware CEO Pat Gelsinger: “VMware is pleased to provide support for Clean Path. We intend to create end-to-end 5G infrastructure that is open, secure, programmable, reliable, and software driven. Safety and security should be the goal of everybody globally who is serious about building the best and safest possible telecommunications infrastructure for 5G, 6G, and beyond.”

Momentum for The Clean Network initiative is growing. The United States calls on our allies and partners in government and industry around the world to join the growing tide to secure our data from the CCP's surveillance state and China's Great Firewall, where data comes in but does not flow out and, reciprocally, propaganda goes out, but the truth doesn't come in. By

building a coalition of partners, we will enhance the protection of our citizens' data and our freedoms.

Get more information on The Clean Network: <https://2017-2021.state.gov/5g-clean-network/>

Executive Order on Addressing the Threat Posed by TikTok:

<https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/>

Executive Order on Addressing the Threat Posed by WeChat:

<https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/>

Find out more about American economic diplomacy, headed by Under Secretary of State Keith Krach: <https://2017-2021.state.gov/bureaus-offices/under-secretary-for-economic-growth-energy-and-the-environment/>

TAGS

Cyber Security

Data Collection

Office of the Spokesperson

Security

Security-Building Measures

Technology

Telecommunications



Related Articles

— JANUARY 19, 2021

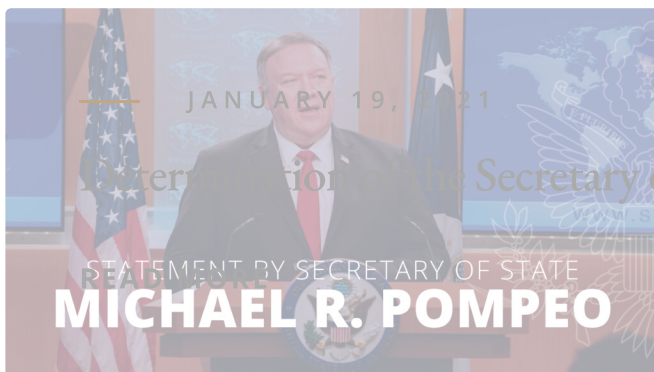
Fulbright Program Partners with National Archives on New Heritage Science Fellowship

[READ MORE](#)

— JANUARY 19, 2021

Secretary Michael R. Pompeo With John Roberts of Fox News America Reports

[READ MORE](#)



Statement of the Secretary of State on Atrocities in Xinjiang

STATEMENT BY SECRETARY OF STATE
MICHAEL R. POMPEO

White House

USA.gov

Office of the Inspector General

[Archives](#)
[Contact Us](#)



[Privacy Policy](#)

[Accessibility Statement](#)

[Copyright Information](#)

[FOIA](#)

[No FEAR Act](#)