ITA Publication No.: CIO 19-G-SEC-004	Revision Date: 06/05/2019
Effective Date: 06/05/2019	

PROHIBITED SOFTWARE GUIDANCE

1. PURPOSE

To establish guidelines for prohibited software due to risks inherent in the supply chain, design, implementation, and/or corporate control of certain software it presents a significant risk to the cyber posture of the ITA TSI wants to ensure that ITA staff can protect themselves and allows the use of certain applications for appropriate purposes.

2. BACKGROUND

The Chief Information Security officer (CISO) is responsible for developing and implementing an information security program which includes creating guidance documents designed to protect enterprise communications, systems, and assets from both internal and external threats. In conjunction with the Chief Information Officer (CIO), the TSI CISO works to procure cybersecurity products and services and to manage disaster recovery and business continuity plans. The CISO anticipates new threats and actively works to prevent them from occurring by establishing directives, guidance, and procedures.

3. SCOPE AND APPLICABILITY

This guidance applies to all ITA organizational units and their employees, federal and contractors, guests, collaborators, and other personnel requiring access to the hardware and software components that constitute ITA's IT systems.

4. GUIDANCE

TSI maintains a list of prohibited software. The software on this list is not allowed to be executed or installed on any Government Furnished Equipment (GFE) information processing devices, including servers, desktops, laptops, tablets, cellular phones, or any other information processing asset. In certain cases an exemption may be documented and approved by the CIO, however no exceptions to this policy are to be allowed without the express written permission of the CIO.

This guidance is subordinate to and does not supersede the directions for protecting Personally Identifiable Information, Business Identifiable Information, and other sensitive information as spelled out in ITA, DOC, and Federal policies.

All software on this list is prohibited from being used or installed on Government Furnished Equipment (GFE) at ITA:

a) Waze
b) WeChat

5. RELATED DOCUMENTS

A. ITA Rules of Behavior for Network Access (http://itacentral/ita/ocio/Shared Documents/ITA Rules of Behavior for Network Access.pdf)
B. The Department of Commerce Office of the Secretary General Rules of Behavior (https://connection.commerce.gov/agreements/office-secretary-general-rules-behavior-users)
C. Use of Personal E-Mail for Official Communication Prohibited (https://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2014/personal_email_for_official_communication_prohibited_2013_05_28.pdf)

WAIVERS

There are no waivers for this guidance.

6. ADDITIONAL INFORMATION

For further information about this guidance, contact the IT Security Office at ITA.

7. AUTHORITY

A. The Federal Information Security Modernization Act of 2014
B. Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. § 1401)
C. Computer Security Act (1987): https://www.congress.gov/bill/100th-congress/house-bill/145

8. MATERIAL SUPERSEDED

N/A

Joe Ramsey
Chief Information Security Officer
Technology, Services and Innovation
International Trade Administration