| ITA Publication No.: CIO 19-G-SEC-001 | Revision Date: 06/05/2019 |
|---|---|
| Effective Date: 06/05/2019 | |

# USING ENCRYPTED MESSAGING SERVICES GUIDANCE

## 1. PURPOSE

To establish guidelines for acceptable use of encrypted messaging services. Proper use of encrypted messaging services will ensure the physical safety of ITA staff. 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 only authorizes the use of encrypted messaging services from American companies that use sufficiently strong encryption.

Examples of acceptable use of encrypted messaging services include:

a) Coordinating arrivals and departures with ITA staff, partners, and clients while traveling abroad.
b) Unofficial communications for the purposes of managing event or travel logistics and other coordination activities.

Examples of **unacceptable** use of encrypted messaging services include, but is not limited to:

a) Sending, distributing, or retaining fraudulent, harassing, obscene or sexually explicit material messages and/or materials.
b) Engaging in private commercial business activities or profit-making ventures.
c) Creating, using, accessing, downloading, storing, or distributing any copyrighted materials that are not properly licensed by the Government for official use on ITA IT systems. This includes but is not limited to audio, video, still images, and software files.

d) Incurring additional costs to the Government.
e) Sharing passwords.
f) Gambling.
g) Sending, distributing, or retaining substantive documents.
h) Conducting Official Business or generating, sending, distributing, or retaining Official Records.
i) Engaging in conduct unbecoming a representative of the Government, or any other behavior that would embarrass the Government.

Approved encrypted messaging products:
a) Signal

Prohibited Encrypted messaging products:
a) 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

CIO Policy 17-14 Using Encrypted Messaging Services, 2017-08-18

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