Information Technology Security Oversight Policy

Policy Number: P-002

Last Updated: 2021-04-15

REVISION HISTORY

Date	Version	Description of Change	Author
02/15/2019	0.1	Creation of IT Security Policy	Lois Mockabee
05/22/2019	0.2	Managerial Edits	Joe Ramsey
06/28/2019	0.3	Included DOC ITSBP document	Tim McGrail
06/28/2019	0.4	Baseline document for signature	Tim McGrail
08/24/2019	0.5	Administrative edits to item B	Tim McGrail
11/06/2019	0.6	Added 0-day vulnerability language	Tim McGrail
12/11/2019	0.7	Reformatted for Appendixes	Tripp Duke
12/12/2019	0.8	2019 Final for signature by Acting CIO	Tim McGrail
04/21/2020	0.9	Incorporated new guidance documents	Tripp Duke
04/21/2020	1.0	Final for signature by Acting CIO 00	Tripp Duke
04/22/2020	1.1	Editorial change to CIO Signature	Lois V. Mockabee
01/14/2020	1.2	Added WhatsApp to the list of prohibited Apps	Shown Horton
04/13/2021	1.3	Removed WhatsApp from the list of prohibited Apps	Lois V. Mockabee
04/15/2021	1.4	Transferred information into approved policy template	Shown Horton

TABLE OF CONTENTS

ACQUISITION OVERSIGHT POLICY

PURPOSE

The International Trade Administration (ITA) Information Technology (IT) Security Policy document specifies and explains the minimum standards for implementing IT security policies and procedures within ITA and thereby establishes the foundation for comprehensive rules and practices that regulate access to the ITA's IT systems, and the information processed, stored, and transmitted by those systems.

BACKGROUND

Cybersecurity is one of the most daunting challenges facing agencies in the United States Federal Government. Though the International Trade Administration (ITA) has staff distributed across the entire globe, the organization is committed to protecting the information that is critical to every employee.

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. Finally, it is imperative that the CISO monitors compliance with all security directives to ensure that it is widely implemented and allows the ITA be pro-active when it comes to ensuring the integrity of our computing infrastructure.

SCOPE AND APPLICABILITY

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.

ORIGINATOR

TSI, Office of the Chief Information Officer.

POLICY

- The CISO shall serve as the CIO's liaison to federal agencies for all matters relating to ITA's IT security.
- The CISO shall enforce compliance of the ITA Rules of Behavior and will develop additional ITA procedures and guidance documents for implementing information security technologies.
- All ITA employees and contractor employees are entrusted with ensuring the cyber-security posture of ITA computing devices.
- All computing devices (desktop computer, laptop, or phone) shall be connected to the ITA network within 24 hours of notification by TSI of a 0-day vulnerability and shall remain connected for a period at least 24 hours.

Using Encrypted Messaging Services

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:

- Coordinating arrivals and departures with ITA staff, partners, and clients while traveling abroad.
- 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:

- Sending, distributing, or retaining fraudulent, harassing, obscene or sexually explicit material messages and/or materials.
- Engaging in private commercial business activities or profit-making ventures.
    - 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.
- Incurring additional costs to the Government.
- Sharing passwords.
- Gambling.
- Sending, distributing, or retaining substantive documents.
- Conducting Official Business or generating, sending, distributing, or retaining Official Records.
- Engaging in conduct unbecoming a representative of the Government, or any other behavior that would embarrass the Government.

Approved encrypted messaging products:

- Signal

Prohibited encrypted messaging products:

- WeChat

Account Access

ITA has the right to monitor the employees' use of their accounts and must ensure that all personnel who use these accounts are aware of this fact. Upon logging on to any ITA computer system, all employees are informed that usage may be monitored, recorded, read, copied, and disclosed by and/or to authorized personnel for official purposes, including criminal investigations and that there is no expectation of privacy. Access or use of the ITA computer system by any person, whether authorized or not, constitutes consent to these items. There is a myriad of specific instances for Directors, Supervisors, System Administrators, and/or individuals acting on their behalf to access the accounts of ITA employees. These occurrences are, but not limited to, a criminal investigation, an unexpected passing of the employee, and/or the need by an authorized individual to access time-sensitive material on the employee's account.

Examples of Instances Requiring Access to Employee Accounts (Not All-Inclusive):

- **Criminal Investigation:** The actions of Federal employees might result in a reprimand or firing. Allegations of misconduct for federal employees can involve both internal civil and administrative investigations along with criminal proceedings. While criminal investigations related to federal employee misconduct may begin at the same time as an internal administrative investigation, they must be handled like any other criminal investigation. Once ITA is notified that an employee is under any investigation, the appropriate adjudicating authority may compel access to all government accounts used by the individual suspected of the offense
- **Passing of an Employee:** If a current or former ITA employee has passed, ITA can access all accounts used for official business-related purposes.
- **Time-Sensitive Requirement:** If a superior has requested a deliverable that is needed immediately from an employee who is incapacitated and cannot immediately access their ITA account, a Superior may require access to their account to retrieve the specific item. Superiors are defined as Political Appointees, Senior Executive Services Members, and other Key Staff.
- **FOIA Request:** Under the FOIA, agencies must disclose any information that is requested except to the extent that such records (or portions of them) are protectable from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.

All ITA Employees have acknowledged this document based on their consent to monitoring on the start-up page and the annually signed Accepted Rules of Behavior memorandum. Additionally, the Federal Records Act (Code of Federal Regulations (CFR) 36 and 44 USC), generally requires agencies to keep and organize electronic messages relevant to agency business as official agency documents, subject to disclosure under the Freedom of Information Act (FOIA) and for other purposes. All ITA staff, including key staff, must adhere to all applicable records management policies, including those defined by their Business Unit (BU), the ITA, and the National Archives and Records Administration.

Prohibited Software

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 installed on Government Furnished Equipment (GFE) at ITA:

- Waze
- WeChat
- Zoom

ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Chief Information Officer (CIO)or Deputy Chief Information Officer (DCIO)	• Ensures that all IT Investments adhere to federally mandated requirements and to the requirements stipulated in the TSI Policies for Capital Planning Investment and Control (CPIC), Enterprise Architecture (EA), Security, and Records Management. • Ensures IT security actions are consistent with CIO-approved plans and strategies • Coordinates with CISO on all security plans, procedures, and policies
TSI Chief Information Security Officer (CISO)	• Develops and implements information security program. • Creates guidance documents designed to protect enterprise communications, systems, and assets from both internal and external threats. • Works to procure cybersecurity products and services and to manage disaster recovery and business continuity plans. • Anticipates new threats and actively works to prevent them from occurring by establishing directives, guidance, and procedures.
Directorates	• Ensures that security policies, protocols and procedures are adhered to. • Ensures that the proper security training is completed.

REFERENCES

TSI Guidance

- Using Encrypted Messaging Services Guidance, G-SEC-001, TSI, June 2019
- Government Furnished Equipment Security Update Guidance, G-SEC-002, TSI, June 2019
- Account Access Guidance, G-SEC-003, TSI, June 2019
- Prohibited Software Guidance, G-SEC-004, June 2019 ITA Rules of Behavior for Network Access
- Use of Personal E-Mail for Official Communication Prohibited

DOC Documents

- Final DOC IT Security Baseline Policy, 06-24-2019
- Commerce Information Technology Requirements Board (CITRB): TBD
- NIST 800 Series Special Publications – 800-53
- The Department of Commerce Office of the Secretary General Rules of Behavior

WAIVERS

There are no waivers for this policy.

ADDITIONAL INFORMATION

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

MATERIAL SUPERSEDED

- TSI IT Security Policy (December 2019)
- CIO Policy 17-14 Using Encrypted Messaging Services, 2017-08-18

RONA BUNN

Digitally signed by RONA BUNN
Date: 2021.04.16 10:36:07 -04'00'

Rona Bunn
Chief Information Officer
Technology, Services and Innovation
International Trade Administration

APPENDIX A: Definition of Terms

Chief Information Officer (CIO) - The person within the ITA accountable for information technology (IT) management. This role may be delegated down to directors who are responsible for IT management within a directorate.

Chief Information Security Officer (CISO) - 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.

Deputy Chief Information Officer (DCIO) - Provides leadership and guidance in critical areas of technology administration in ITA, including budgeting, resource development and allocation, policy formation, technology evaluation, and service development, delivery, and deployment. Acts on behalf of the CIO as assigned by the CIO or in the absence of the CIO as the principal IT officer on executive decisions and executive level committees.

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

APPENDIX B: Acronyms

Acronym	Term
BU	Business Unit
CCA	Clinger-Cohen Act of 1996
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSSP	Committee on National Security Systems Policy
DOC	Department of Commerce
FISMA	Federal Information Security Management Act of 2002
FITARA	Federal Information Technology Acquisition Reform Act of 2014
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
IA	Information Assurance
IT	Information Technology
ITA	International Trade Administration
NARA	National Archives and Records Administration
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OS	Office of the Secretary
PRA	Paperwork Reduction Act
USC	United States Code

APPENDIX C: Legal Authorities and Guidance

Legislation

- Federal Cybersecurity Workforce Strategy
- Clinger-Cohen Act (CCA) of 1996, P.L. 104-106
- Federal Information Technology Acquisition Reform Act (FITARA)
- Chief Financial Officers Act of 1990 (Public Law 101-576)
- Federal Information Security Modernization Act of 2014 (FISMA)
- Computer Security Act (1987):
- Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35)
- Information Technology Management Reform Act of 1996 (40 U.S.C. §1401)
- E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. Chapter 36)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)

National Policy, Directives and Memorandum

- OMB Circular A-130, "Management of Federal Information Resources"
- President's 2018 Management Agenda
- Executive Order 13800 , **"**Federal IT Modernization"
- The Federal Risk and Authorization Management Program (FedRAMP)
- Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 2012
- Committee on National Security Systems Policy (CNSSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, July 2003
- Code of Federal Regulations, Title 5, Administrative Personnel, Section 731.106
- Designation of Public Trust Positions and Investigative Requirements (5 C.F.R. 731.106)
-

Department of Commerce

- Final DOC IT Security Baseline Policy, 06-24-2019
- Commerce Information Technology Requirements Board (CITRB): TBD
- NIST 800 Series Special Publications – 800-53

International Trade Administration

- Using Encrypted Messaging Services Guidance, G-SEC-001, TSI, June 2019
- Government Furnished Equipment Security Update Guidance, G-SEC-002, TSI, June 2019
- Account Access Guidance, G-SEC-003, TSI, June 2019
- Prohibited Software Guidance, G-SEC-004, June 2019

APPENDIX D: Security Guidance

USING ENCRYPTED MESSAGING SERVICES GUIDANCE

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.

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.

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.

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:

- Coordinating arrivals and departures with ITA staff, partners, and clients while traveling abroad.
- 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:

- Sending, distributing, or retaining fraudulent, harassing, obscene or sexually explicit material messages and/or materials.
- Engaging in private commercial business activities or profit-making ventures.
- 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.
- Incurring additional costs to the Government.
- Sharing passwords.
- Gambling.
- Sending, distributing, or retaining substantive documents.

- Conducting Official Business or generating, sending, distributing, or retaining Official Records.
- Engaging in conduct unbecoming a representative of the Government, or any other behavior that would embarrass the Government.

Approved encrypted messaging products:

- Signal

Prohibited encrypted messaging products:

- WeChat

RELATED DOCUMENTS

- ITA Rules of Behavior for Network Access
- The Department of Commerce Office of the Secretary General Rules of Behavior
- Use of Personal E-Mail for Official Communication Prohibited

WAIVERS

There are no waivers for this guidance.

ADDITIONAL INFORMATION

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

AUTHORITY

- The Federal Information Security Modernization Act of 2014
- Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. §1401)
- Computer Security Act

MATERIAL SUPERSEDED

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

ACCOUNT ACCESS GUIDANCE

PURPOSE

To provide International Trade Administration (ITA) Account Access guidance.

BACKGROUND

Title I of the Federal Electronic Communications Privacy Act of 1986 (18 United States Code (USC) Sections 2510, 2701, and 3121) states that any workplace correspondence on a government device is the property of the employer. At ITA, any government-furnished equipment supplied to an employee is the property of ITA and shall be used for authorized purposes or according to guidance in the limited personal use policy. Accessing an employees' account may be needed to secure evidence in the case of a lawsuit or the government may want to monitor the e-mails of an employee suspected of sending proprietary or inappropriate information to outside agencies. The Account Access Policy protects ITA from legal liability, reputation damage, and potential security breaches and can be used as a mechanism for ensuring that the workplace is free of harassment. This guidance provides the instances that warrants accessing an employees' account and the steps for obtaining authorization.

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.

GUIDANCE

ITA has the right to monitor the employees' use of their accounts and must ensure that all personnel who use these accounts are aware of this fact. Upon logging on to any ITA computer system, all employees are informed that usage may be monitored, recorded, read, copied, and disclosed by and/or to authorized personnel for official purposes, including criminal investigations and that there is no expectation of privacy. Access or use of the ITA computer system by any person, whether authorized or not, constitutes consent to these items. There is a myriad of specific instances for Directors, Supervisors, System Administrators, and/or individuals acting on their behalf to access the accounts of ITA employees. These occurrences are, but not limited to, a criminal investigation, an unexpected passing of the employee, and/or the need by an authorized individual to access time-sensitive material on the employee's account.

Examples of Instances Requiring Access to Employee Accounts (Not All-Inclusive):

- **Criminal Investigation:** The actions of Federal employees might result in a reprimand or firing. Allegations of misconduct for federal employees can involve both internal civil and administrative investigations along with criminal proceedings. While criminal investigations related to federal employee misconduct may begin at the same time as an internal administrative investigation, they must be handled like any other criminal investigation. Once ITA is notified that an employee is under any investigation, the appropriate adjudicating authority may compel access to all government accounts used by the individual suspected of the offense
- **Passing of an Employee:** If a current or former ITA employee has passed, ITA can access all accounts used for official business-related purposes.
- **Time-Sensitive Requirement:** If a superior has requested a deliverable that is needed immediately from an employee who is incapacitated and cannot immediately access their ITA account, a

Superior may require access to their account to retrieve the specific item. Superiors are defined as Political Appointees, Senior Executive Services Members, and other Key Staff.

- **FOIA Request:** Under the FOIA, agencies must disclose any information that is requested except to the extent that such records (or portions of them) are protectable from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.

All ITA Employees have acknowledged this document based on their consent to monitoring on the start-up page and the annually signed Accepted Rules of Behavior memorandum. Additionally, the Federal Records Act (Code of Federal Regulations (CFR) 36 and 44 USC), generally requires agencies to keep and organize electronic messages relevant to agency business as official agency documents, subject to disclosure under the Freedom of Information Act (FOIA) and for other purposes. All ITA staff, including key staff, must adhere to all applicable records management policies, including those defined by their Business Unit (BU), the ITA, and the National Archives and Records Administration.

RELATED DOCUMENTS

IT Information Management Policy, July 2019

WAIVERS

There are no waivers for this guidance.

ADDITIONAL INFORMATION

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

AUTHORITY

- Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35)
- Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. §1401)
- E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. Chapter 36)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)

MATERIAL SUPERSEDED

N/A

PROHIBITED SOFTWARE GUIDANCE

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.

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.

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.

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:

- Waze
- WeChat
- Zoom

RELATED DOCUMENTS

- IT Information Management Policy, July 2019
- ITA Rules of Behavior for Network
- The Department of Commerce Office of the Secretary General Rules of Behavior

WAIVERS

There are no waivers for this guidance.

ADDITIONAL INFORMATION

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

AUTHORITY

- Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35)
- Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. §1401)
- Computer Security Act (1987)

MATERIAL SUPERSEDED

N/A