ITA Publication No.: CIO 19-G-SEC-002	Effective Date: 6/05/2019
Revision Date: 8/24/2019	

GOVERNMENT FURNISHED EQUIPMENT (GFE) SECURITY UPDATE GUIDANCE

1. PURPOSE

To establish the guidance for International Trade Administration (ITA) end users to connect all ITA Government Furnished Equipment (GFE) to the network to receive the latest security and network updates.

2. BACKGROUND

Security updates are a vital component of running antivirus[1] and firewall[2] software for computers. To minimize the number of computer security incidents related to malware[3] and disruption, ITA is being proactive to ensure the integrity of our computing infrastructure.

3. SCOPE AND APPLICABILITY

This guidance applies to all users issued ITA GFE.

4. GUIDANCE

A. All computing devices (desktop computer, laptop or phone) shall be connected to the ITA network (either onsite or via Virtual Private Network[4] (VPN)) every week and shall remain connected for a period at least 24 hours to ensure that the latest cyber security patches are downloaded and properly installed. The end user is responsible for ensuring that the device is connected and allowing enough time for the patching activities to occur.

B. All ITA software updates shall be installed by Enterprise Operations.

5. RELATED DOCUMENTS

A. IT Information Management Policy, 2019
B. IT Security Policy, 2019
C. Working Remotely with GFE at ITA
D. Citrix Quick Reference Sheet
E. ITA Rules of Behavior
F. Draft Antivirus and Malware Compliance Procedures (CIO SXXX)
G. Committee on National Security Systems Instruction No. 4009 (April 6, 2015)
H. Federal Trade Commission, How Not to Get Hooked by a "Phishing" Scam (March 6, 2017)

[1] "Antivirus" is software designed to detect and destroy computer viruses.
[2] "Firewall" is the part of a computer system or network which is designed to block unauthorized access while permitting outward communication.
[3] "Malware" is short for "malicious software" which are computer programs designed to infiltrate and damage computers without the users consent. Malware includes viruses, worms, Trojan Horses, rootkits, and spyware.
[4] "Virtual Private Network" is a network that is constructed using public wires (usually the internet) to connect remote users or regional offices to a company's private, internal network.

I. National Cybersecurity and Communications Integration Center (NCCIC) (April 2019)

6. WAIVERS

There are no waivers from this document.

7. ADDITIONAL INFORMATION

For further information about this document, contact the Policy and Strategic Planning Directorate at ITA.

8. AUTHORITY

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

9. MATERIAL SUPERSEDED

N/A

APPROVED BY:

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