2019-02-008

Republic of the Philippines
Department of Finance
BUREAU OF CUSTOMS
1099 Manila

MEMORANDUM

TO : **DEPUTY COMMISSIONER, MISTG**
ALL DIRECTORS
DISTRICT COLLECTORS
ALL DIVISION CHIEFS

FROM : **REY LEONARDO B. GUERRERO**
Commissioner

SUBJECT : **SECURING COMPUTERS/ INTER-NETWORKS BEING USED FOR E2M APPLICATION**

DATE : **JANUARY 31, 2019**

Section 109 of Republic Act No. 10863, otherwise known as the Customs Modernization and Tariff Act (CMTA), mandates the Bureau of Customs to ensure that "the security of data and communication shall be in a manner that is consistent with applicable local and internationally accepted standards on information security."

In line with the foregoing, and to protect confidential data contained inside our Electronic to Mobile (E2M) system, the following procedures and policies shall be observed:

A. Downloading of information from the E2M shall require the approval of the Commissioner, thru the Deputy Commissioner of MISTG. Thus, requests for data download from the E2M shall be done in writing, and to be endorsed by the Deputy Commissioner of MISTG, to the Commissioner.

B. To further secure the computing environment, the Deputy Commissioner of MISTG is tasked to monitor compliance with, and whenever possible, to employ technological tools to enforce the following:

   1. Only BOC issued desktops and laptops shall be used to access E2M. E2M SAD and other Customs documents may be printed from E2M Computers.

   2. Computers used for E2M access (E2M Computers) should not be able to access the social media sites, non-BOC emails, proxy sites, and other websites that can allow transfer of information (such as file-sharing sites, peer-to-peer applications, etc).

3. USB ports (all types) of E2M Computers shall be used only for keyboard, mouse and printers. All other uses of USB ports in E2M Computers shall be disallowed.

4. PDF copies of Customs documents in E2M can be sent out only through the BOC official email.

5. MISTG shall ensure, through available technology controls, that data inside E2M computer terminals cannot reach any other network storage device.

6. The computer hard disks used by E2M Computers shall be secured and properly marked to make it identifiable in cases of theft.

7. Remote access to E2M Computers using terminal services, remote desktop applications or any similar applications such as TeamViewer, VNC, etc. are strictly prohibited.

8. Installation of any other application that can be used to harvest data from E2M workstations such as keyloggers, XML downloaders, PDF converters, etc. shall be prohibited. This list may be expanded by the Deputy Commissioner of MISTG.

9. When using VPN, the VPN network settings shall be such that all data transmissions can be monitored, and that the VPN resource cannot be used in any other manner than to connect only to E2M.

10. All BOC Desktops and Laptops shall be joined to the BOC Active Directory, and shall be monitored for proper use.

C. In order to effectively manage information, district collectors shall report all internet connectivity being used by their offices to MISTG. Whenever possible, MISTG shall ensure these internet connections are placed behind the Bureau's firewall. District Collectors and MISTG shall endeavor to disconnect at the soonest possible time, all inter-network connections that are not possible to be placed behind the Bureau's firewall. Until such time, MISTG and all District Collectors and heads of offices shall isolate these internetworks and ensure they are not used to transmit data without prior approval.