MASTER COPY

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

CUSTOMS MEMORANDUM ORDER

NO. 04 - 2019

SUBJECT: **FURTHER DEFINING THE ROLES AND RESPONSIBILITIES OF EACH ORGANIZATIONAL UNIT WITHIN MISTG AS MANDATED UNDER EO 463, AMENDING FOR THE PURPOSE CMO 33-1998, AND SEGREGATING ADMINISTRATOR / PRIVILEGED ACCESS TO MISTG PERSONNEL BASED ON THEIR FUNCTIONS**

Executive Order 463 signed by H.E. Pres. Fidel V. Ramos on January 9, 1998 created the Management Information Systems Technology Group (MISTG). Thereafter, Customs Memorandum Order (CMO) 33-1998 was issued on August 25, 1998 to operationalize EO 463. The CMO enumerated the duties and responsibilities of the two (2) services under MISTG namely: Technology Management Service (TMS), and Planning and Systems Development Service (PSDS). However, there is no CMO issued prescribing the duties and functions of each of the four divisions under MISTG created by EO 463.

Good practices in Information and Communications Technology (ICT) Management calls for stricter control of privileged or administrator access of MISTG personnel by segmenting ICT privileged access to critical elements of the infrastructure. Privileged / administrator access should be given on a strictly per need basis as defined by the personnel, and the personnel's organizational unit's functions, duties and responsibilities. For this purpose, it is necessary that we define each of MISTG's organizational units' functions. *This CMO amends CMO 33-1998 and further clarifies the duties and responsibilities of all organizational units under MISTG, including the four divisions.*

Section 1. Duties and responsibilities of the Technology Management Service (TMS) and the Divisions under it.

1.1. *Technology Management Service* (TMS) shall be responsible for managing the ICT infrastructure including managing the operational aspects of the ICT systems in the Bureau. TMS shall ensure that all systems are working within the appropriate Service Level Agreement (SLA), and shall maintain a tiered response team that will answer and resolve issues within the agreed timelines.

Under the TMS are two divisions, namely the Systems Management Division (SMD), and the Technical Support Division (TSD).

1.2. *Systems Management Division (SMD)* shall be responsible for building, planning and maintaining the Bureau's ICT infrastructure. SMD shall ensure that the ICT infrastructure's capabilities are appropriate to accommodate the needs of the various applications and systems in the Bureau. SMD shall be responsible for the following:

1.2.1. Management of the ICT infrastructure for strategic ICT systems such as (but not limited to) the Bureau's Customs Processing System (CPS), Enterprise Resource Planning (ERP) application, Communications, document management system, office productivity suites, etc.

1.2.2. ICT Facilities Management.

1.2.3. Information Security Management.

1.2.4. Systems and network administration.

1.2.5. Capacity planning of the ICT infrastructure such as network, storage, computing, and other elements of the infrastructure.

1.2.6. Build, and maintain, the infrastructure for the Bureau's ICT Disaster Recovery, and ICT Disaster Response Plans.

1.3. *Technical Support Division (TSD)* shall be the ICT operation arm of MISTG. TSD shall document all issues, and proactively monitor the performance of the entire ICT ecosystem of the Bureau. TSD shall respond to all service requests and request for information thru its "helpdesk". TSD shall also ensure that all incidents and problems are resolved within agreed SLAs, and ICT assets are properly accounted.

1.3.1. Incident Management – TSD shall maintain a Tier 1 and Tier 2 helpdesk for fulfillment of service requests, and troubleshooting reported ICT incidents of the Bureau. The ICT infrastructure within the scope of TSD includes all end-user computing devices (desktops, laptops, IP telephony. Mobile computers, etc.), computing peripherals (printers, scanners), productivity applications, and the Customs Processing System (CPS) application (currently E2M).

1.3.2. Conduct Bureau-wide training, awareness and information drives regarding MISTG program and proper use of ICT equipment and software with focus on developing an ICT security awareness for Bureau personnel.

1.3.3. In relation to section 1.2.2, the Technical Support Division shall train and develop organic personnel of the enforcement and

intelligence units of the Bureau in the use of specialized communications and IT equipment, as well as use of ICT systems relevant to the specific needs of the Bureau's enforcement and intelligence units.

1.3.4. ICT Asset Management from acceptance of procured ICT systems (hardware and software), keeping an inventory of all assets during their lifetime, up to retirement and proper disposal of the asset.

1.3.5. Proactive monitoring of all ICT assets and system performance.

1.3.6. Provide accurate and timely data being captured by the CPS, ERP and other ICT systems to officials of the Bureau, international partners, and other duly recognized external stakeholders/

1.3.7. Certify the integrity of the data as extracted from the Bureau's databases. Said certification shall only certify that the extracted data, as it appears in paper or any medium the data was transmitted, is the same as the data stored in the Bureau's CPS, ERP, and other application's databases being requested.

1.4. *Port Data Management Unit (PDMU)* – shall be composed of all MISTG personnel assigned to various ports and sub-ports of the Bureau. They shall serve as the on-site technical support of the Bureau. Each port PDMU shall be led by at least one designated "Site Team Leader". All Site Team Leaders in the PDMU report directly to the TMS Director.

Section 2. Duties and responsibilities of the Planning and Systems Development Service (PSDS) and the Divisions under it.

2.1. *Planning and Systems Development Service (PSDS)* shall primarily be responsible for developing the ICT best practices for the Bureau, auditing compliance of MISTG, and the Bureau to relevant laws, rules and regulations governing information, information management and information security. PSDS shall also develop the MISTG Information Systems Strategic Plan (ISSP), ensure that procurements of ICT assets are in order, and properly manage ICT projects. PSDS shall likewise develop the Bureau's Software Development Life Cycle (SDLC), ICT incident management processes, risk management processes, and information management processes. Under the PSDS are two divisions namely the Systems Development Division (SDD) and Planning of Information Management Division (PIMD).

2.2. *Systems Development Division (SDD)* shall be responsible for business analysis, requirements gathering, and quality management of systems and software that will either be developed or procured by the Bureau. SDD shall develop the Software Development Life Cycle (SDLC) that is

congruent to developing secure quality robust software solutions quickly for the Bureau. They shall also be responsible for the following:

2.2.1. Administration, maintenance, operation and optimization of the databases of the Bureau's CPS and ERP systems.

2.2.2. Software development and maintenance of its in-house developed software throughout its lifecycle.

2.2.3. Business analysis and requirements management of any strategic ICT projects in the Bureau.

2.2.4. Ensuring that our software development, procurements, and accreditation of ICT systems and services meet the requirements and expectations of all stakeholders.

2.3. *Planning and Management Information Division (PMID)* shall primarily be responsible for managing all strategic procurements of the Bureau relevant to MISTG, preparing the budget in accordance to the strategy formulated relevant to MISTG, staff development, overall project management, PIMD shall also be responsible for the following:

2.3.1. Project Management;

2.3.2. Audit compliance of MISTG to standards and procedures adopted by MISTG, along with existing ICT rules, regulations and statutory requirements of the Bureau;

2.3.3. Document the Bureau's Information Systems Strategic Plan (ISSP) and ensure that the ISSP resource requirements are properly planned, phased, and acquired.

2.3.4. Develop the Bureau's ICT processes such as but not limited to: information security management, data and information management, incident management, risk management, etc. in accordance with industry best practices.

2.3.5. Develop, document, and manage implementation, of the ICT portion of the Bureau's Disaster Recovery and Disaster Response Plans subject to the approval of the Commissioner of the Bureau of Customs.

Section 3. Realignment of Personnel. In lieu of this CMO, a realignment of assignments of existing IT personnel may be prescribed in a separate Customs Personnel Order (CPO) to be issued for the purpose.

Section 4. Rules in granting privileged / administrator access to ICT services. Recognizing the significant risk to confidentiality, integrity, and availability of unmonitored privileged access of our personnel to any ICT infrastructure or system elements, the Deputy Commissioner of MISTG is hereby instructed to:

MASTER COPY

4.1. Ensure that privileged or administrator access of MISTG personnel are limited to only what is necessary, and strictly conforms to the duties and responsibilities outlined in this memorandum order.

4.2. No personnel shall have privileged access to the CPS and ERP in all three elements namely: (a) operating system, (b) database, and (c) software application.

4.3. Access of any BOC personnel to all datacenters are hereby revoked. The Deputy Commissioner for MISTG shall limit access to datacenter to only one person at any given shift and only to access it in emergency situations. All access to datacenters shall be provided only when necessary and only upon written approval of the Deputy Commissioner for MISTG. Such approval shall only be granted for a limited time period. The Deputy Commissioner for MISTG shall also ensure that datacenter access is covered by CCTV surveillance and entry and exit of any personnel is properly recorded.

4.4. In relation to section 4.3. the Deputy Commissioner of MISTG shall ensure that data centers are secured, and a guard is stationed in the data centers' premises 24/7. Entry to the data centers shall be properly vetted and logged in a logbook by the stationed guards.

4.5. System accounts with privileged access rights shall be documented and shall never be used for access by any personnel.

Section 5. Compliance. The Deputy Commissioner for MISTG is hereby directed to report to the Commissioner the steps taken to comply with this memorandum order.

Section 6. Repealing Clause. This CMO amends CMO 33-1998 and previously issued CMOs which are inconsistent with the provisions here stated.

Section 7. Separability Clause. If any part or provision of this Order is later on declared invalid of illegal, the remaining portion shall remain valid and unaffected.

Section 8. Effectivity Clause. This CMO shall take effect immediately and shall last until revoked.

REY LEONARDO B. GUERRERO
Commissioner
FEB 07 2019

Bureau of Customs
Office of the Commissioner
19-03791