DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

Canc: Dec 2020

MCBUL 4000
EGEM
27 NOV 2019

MARINE CORPS BULLETIN 4000

From: Commandant of the Marine Corps
To: Distribution List

Subj: ACCESS MANAGEMENT AND INTERNAL CONTROLS FOR ELECTRONIC COMMERCE SYSTEMS

Ref: See Enclosure (1)

Encl: (1) References

1. Situation

a. Federal agencies have become increasingly dependent on using electronic commerce (e-commerce) systems to acquire goods and services. Although e-commerce facilitates operational efficiency, the lack of established user access internal controls and management oversight increases the risk of fraud, waste, and abuse. Accordingly, this Bulletin establishes policy and internal controls for managing user access to e-commerce systems in compliance with references (a) through (d).

b. E-commerce definition. Per reference (e), e-commerce is the interchange and processing of information using electronic techniques for accomplishing business transactions (i.e., acquire goods and services) based upon the application of commercial standards and practices. E-commerce systems draw on technologies such as mobile commerce, electronic funds transfer, internet marketing, online transaction processing, Electronic Data Interchange (EDI), inventory management systems, and automated data collection systems.

2. Mission. Establish clear roles, responsibilities, and procedures in order to ensure effective access management and internal controls over e-commerce systems. This Bulletin is in accordance with references (a) through (w).

3. Execution

a. Commander’s Intent and Concept of Operations

(1) Commander’s Intent

(a) Establish Marine Corps policy for access management and internal controls over e-commerce systems utilized by the Marine Corps. This will strengthen end-to-end requisition management, to include those actions

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

that result in or result from procurement activities, while meeting the standards and requirements established in references (a) through (j).

(b) Marine Corps E-commerce systems. This Bulletin will focus on managing e-commerce systems with the greatest impact on the Marine Corps accounting system, Standard Accounting, Budget, and Reporting System. This includes: Global Combat Support System - Marine Corps (GCSS-MC), Purchase Request Builder (PR Builder), Procurement Integrated Enterprise Environment (PIEE) – Wide Area Work Flow (WAWF), Federal Mall/Electronic Mall, General Services Administration Advantage, and USMC ServMart virtual web site (ServMart online).

(2) Concept of Operations. Effective use of e-commerce systems requires the establishment of effective user access controls, management oversight, and system advocacy. This Bulletin codifies necessary roles and responsibilities of unit-level Commanding Officers/Accountable Officers (CO/AO), higher echelons throughout the chain of command, and Headquarters Marine Corps (HQMC) system advocates. Per reference (k), the term CO/AO refers to a commander, Commanding General (CG), Commanding Officer (CO), or accountable officer (AO) with requisition authority (Authority Code “00” Department of Defense Activity Address Code (DoDAAC)) that operates under U.S. Code Title 10/31.

(a) User Access Controls. E-commerce user access controls consist of two components: (1) *User system access* in which a user is granted access to a respective e-commerce system, and (2) *user role/permission assignment* in which a user is granted system-specific roles and permissions commensurate with appointed authorities. Most e-commerce systems used by the Marine Corps have a unique role title for the individual who manages “access rights” for the users in a given system (e.g., Unit User Account Manager (UUAM), Government Administrator, Group Access Manager (GAM), System Administrator, disburser administrator, etc.). For the purposes of this Bulletin, this individual will be referred to as the User Access Manager (UAM).

1. Depending on the e-commerce system, the above two components may be accomplished as a single step by an individual administrator (e.g., GCSS-MC UUAM grants user access and assigns roles/permissions at the same time), or they may be divided into two steps executed by two individuals (e.g., PIEE-WAWF users are granted access to the system by a PIEE-WAWF system administer but roles/permissions are added by a command-appointed GAM).

2. For effective user access control, both components must be managed to prevent the potential for fraud, waste, and abuse.

3. Primary responsibility for e-commerce system user access control and management oversight at the lowest level belongs to the CO/AO of commands with requisition authority. This responsibility is delegated to the CO/AO-appointed UAM.

4. User Access Manager (UAM) Responsibilities. UAMs are primarily responsible for performing or coordinating user activation/deactivation and assignment of roles/permissions in e-commerce systems at the unit level. Specific UAM responsibilities include the following.

a. Prior to the activation of any user role, review the user’s DD 2875 “System Authorization Access Request (SAAR)” ensuring that proper reviews and signatures are completed. E-commerce system SAAR forms must be retained for one (1) year following termination of a user's access to the system.

b. Ensure that e-commerce system access requests have documentation supporting the user’s roles/permissions. Depending on the user’s roles/permission, supporting documentation may include a CO/AO appointment letter, DD 577 “Appointment/Termination Record-Authorized Signature", and/or NAVMC 11869 "Notice of Delegation of Authority” identified in references (k), (l), and (n).

c. Per reference (n), ensure users with permissions to fill a certifying officer role (e.g., PIEE-WAWF acceptor or local processing official) complete an approved certifying officer training course applicable to their mission prior to their appointment and activation within the system. Refresher training must be completed annually.

d. Per reference (o), ensure users with permission to execute funds control (e.g., PR Builder supply officer role) complete fiscal/appropriations law training and the online budget execution courses. Reference (n) defines fund control individuals as those who receive or issue Appropriated Funds (APF) or generate purchase requests for APF (e.g., supply, contracting, etc.).

e. If the e-commerce system does not support uploading user documentation, maintain all supporting user access documentation physically or electronically in accordance with document retention requirements established in this Bulletin and reference (l). When a system supports uploading user documentation, ensure all supporting documentation is uploaded prior to granting access to the e-commerce system.

f. Establish and manage check-in and check-out procedures within the unit to ensure deactivation of users prior to departure from the unit (e.g., end of active service, permanent change of station, etc.). Prior to endorsing the user's check-out sheet, UAMs must remove the user’s e-commerce system roles and permissions and disable access to the system.

g. Per reference (p) and as part of the supply officer internal controls review program (reference (q)), perform and document semi-annual e-commerce system user account reviews to ensure user access and account privileges are commensurate with job functions; military or support contractor status are accurate; and user access documentation and training certificates are on file.

(1) E-commerce system users with an identified discrepancy during the review represent a potential risk. Corrective action must be taken to resolve user discrepancies to prevent potential fraud, waste, and abuse.

(2) Evidence of user access reviews must be documented and maintained in accordance with reference (q).

h. For e-commerce system access obtained prior to SAAR completion (e.g., access granted by federal agencies outside the Marine

Corps), ensure that authorized e-commerce system users complete the required user documentation as described in paragraph 3a(2)(a)4 of this Bulletin.

i. Ensure all guest accounts (for private contractor personnel) are sponsored by the appropriate government member of the administrative organization managing the contract (i.e. contracting officer or contracting officer representative). Ensure that valid guest account sponsorship documentation is properly completed and maintained on file.

j. Reset user accounts and re-associate new user certificates as required.

k. As necessary, serve as the command consolidation point for reviewing, vetting, and forwarding respective system Engineering Change Proposals (ECPs) via the chain of command to the HQMC e-commerce system advocate.

(b) Management Oversight. Management oversight responsibilities extend to higher echelon commanders, CGs, or COs throughout the chain of command (e.g., regimental, Major Subordinate Command, Marine Expeditionary Force, and Marine Force-level). These individuals shall leverage their functional end-to-end requisition management subject matter experts (i.e., logisticians) in executing their management oversight responsibilities. Specific responsibilities include the following.

1. Provide management oversight of subordinate organization CO/AO-appointed UAMs.

2. As necessary, serve as the command consolidation point for reviewing, vetting, and forwarding respective system ECPs via the chain of command to the HQMC e-commerce system advocate.

3. Provide coordination, oversight, and enforcement of all e-commerce system issues to include emerging requirements, future initiatives, and external audit findings that result in required action by subordinate organization UAMs.

4. Ensure a semiannual review of subordinate unit e-commerce system UAM accounts is conducted to ensure that UAMs are valid for each e-commerce system.

a. Evidence of UAM reviews must be documented and maintained in accordance with reference (q).

b. Ensure unauthorized UAMs are terminated to prevent potential fraud, waste, and abuse.

5. As dictated by the e-commerce system advocates, some e-commerce systems require a higher echelon UAM (e.g., regimental UAM) to assign subordinate unit UAM roles (e.g., battalion-level UAM role) within the system. In these instances, higher echelons will appoint UAMs to take appropriate action.

6. Facilitate user access support to all subordinate users, to include aspects of both system use and business process requirements of the respective system.

7. Monitor and enforce timely resolution of business event errors received from internal or higher headquarters generated reports (i.e. receiving reports, invoices identified as delinquent, and user access reports).

(c) System Advocacy. In support of commands with requisition authority and their respective higher headquarters, HQMC e-commerce system advocates are assigned to each of the e-commerce systems identified in paragraph 3a(1)(b). Specific responsibilities include the following.

1. Publish user access requirements and instructions for each e-commerce system used by the Marine Corps. At a minimum, provide the following information:

a. Clarification of e-commerce system terminology compared to Marine Corps policy. As an example, an e-commerce system role may be called “approver” which is equivalent to a CO/AO-appointed supply officer and personnel with fund approval authority (DD 577).

b. Clarification of support hierarchies for UAM assignments and management oversight. As an example, a CO/AO-appointed UAM is granted system access to GCSS-MC from the GCSS-MC Program Office; however, system access to PIEE-WAWF is granted from a higher headquarters UAM.

c. Specific instructions for granting and removing user access, roles, and permissions for each e-commerce system.

d. Identification of UAM and user training requirements for each e-commerce system.

2. Coordinate with the program manager for each e-commerce system (Marine Corps systems and non-Marine Corps systems) to develop system specific training for managing system accounts and user access.

3. Ensure an annual review of e-commerce system UAM accounts is conducted to ensure that UAMs are valid for each e-commerce system.

a. Evidence of UAM reviews must be documented and maintained.

b. Coordinate the termination of unauthorized UAMs to prevent potential fraud, waste, and abuse.

4. On a quarterly basis, disseminate user account information to Marine Corps UAMs to facilitate semi-annual user account reconciliations.

5. Coordinate the resolution and timely response of e-commerce error reports.

6. Coordinate appropriate e-commerce system changes (i.e., ECPs) to improve effective management of system accounts and user access.

b. Subordinate Element Missions

(1) Deputy Commandant, Installations and Logistics

(a) Appoint in writing HQMC system advocates for each of the e-commerce systems identified in paragraph 3a(1)(b) to execute the responsibilities listed in paragraph 3a(2)(c).

(b) As necessary, publish Marine Corps specific user access requirements and UAM instructions for each e-commerce system within one year of the release of this Bulletin.

(c) Coordinate with Deputy Commandant, Information (DC I) to ensure the procedures identified in this Bulletin are included in applicable user access management guidance.

(d) Conduct an annual review of e-commerce system UAM accounts to ensure that UAMs are valid for each e-commerce system.

(e) Evaluate compliance of this Bulletin via Internal Controls and Audit Readiness Team or regional Field Supply and Maintenance Analysis Office inspections.

(f) Incorporate the contents of this Bulletin within MCO 4400.201 and reference (q).

(2) Commander, Marine Corps Systems Command

(a) Maintain system oversight of applicable e-commerce systems to ensure effective system controls are in place in accordance with references (c) and (d).

(b) Ensure privileged user access for UAMs is restricted to authorized individuals.

(c) In coordination with the respective HQMC system advocate, ensure compliance with this Bulletin and provide additional guidance as necessary.

(3) Marine Corps Commanders and Accountable Officers

(a) Appoint in writing UAMs for each of the e-commerce systems identified in paragraph 3a(1)b to execute the responsibilities identified in paragraph 3a(2)(a)4.

(b) Ensure compliance with this Bulletin and provide amplifying guidance as necessary.

(c) Revise local Standard Operating Procedures (SOP) to ensure compliance with this Bulletin.

4. Administration and Logistics

a. Records Management. Records created as a result of this Bulletin shall be managed according to National Archives and Records Administration approved dispositions per references (r) and (v) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium. Refer to reference (w) for Marine Corps records management policy and procedures.

b. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended (reference (s)) and implemented per reference (t).

5. Command and Signal

a. Command. This Bulletin is applicable to the Marine Corps Total Force.

b. Signal. This Bulletin is effective the date signed.

C. G. CHIAROTTI
Deputy Commandant
Installations and Logistics

DISTRIBUTION: PCN 10200368000

References

(a) OMB Circular A-123, “Management’s Responsibility for Enterprise Risk Management and Internal Control,” 15 July, 2016
(b) FISCAM, 2 February, 2009
(c) NIST Special Publication 800-53, Revision 4, April, 2013
(d) NIST Special Publication 800-34, Revision 1, May, 2010
(e) DoDD 8190.1, “DoD Logistics Use of Electronic Data Interchange (EDI) Standards,” 5 May, 2000
(f) Under Secretary of Defense (Comptroller)/Chief Financial Officer, Financial Improvement and Audit Readiness (FIAR) Guidance, 3 April, 2017
(g) DoDI 8510.01 CH-2, “Risk Management Framework (RMF) for DoD Information Technology (IT),” 28 July, 2017
(h) SECNAVINST M-5239.2
(i) MCO 5239.2B
(j) MCO 7510.5A
(k) MCO 4400.201 Volume 1
(l) MCO 4400.201 Volume 3
(m) CMC L EGEM Washington DC, 241744Z, January, 2017
(n) DoD 7000.14-R, “Financial Management Regulation,” date varies by volume
(o) MARADMIN 350-11
(p) MCO 5200.24E
(q) NAVMC 4000.5C
(r) SECNAV M-5210.1 CH-1
(s) 5 U.S.C. 552a
(t) SECNAVINST 5211.5F
(u) CMC Washington DC L EGEM 231457Z, September, 2016
(v) SECNAV Notice 5210
(w) MCO 5210.11F