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

MCO 4000.61
I&L (LP)
1 Feb 2024

MARINE CORPS ORDER 4000.61

From: Commandant of the Marine Corps
To: Distribution List

Subj: ELECTRONIC COMMERCE USER ACCESS MANAGEMENT

Ref: See enclosure (1)

Encl: (1) References
(2) Commonly Used Systems
(3) Certification Template

1. Situation

a. The Marine Corps is dependent on the use of electronic commerce (E-commerce) systems to acquire goods and services, both via commercial and federal sources of supply. Although E-commerce facilitates operational efficiency, the lack of established user access controls and codified management requirements throughout the logistics command hierarchy increases the risk of fraud, waste, abuse, mismanagement of resources, loss of property accountability, and a degradation in supply and materials operational readiness. Accordingly, this Order establishes policy and requirements for managing access to E-commerce systems in compliance with references (a) through (q) and implements logistics operational support requirements for E-commerce systems.

b. This Order establishes Marine Corps-specific requirements for the administration of user access for all E-commerce systems used in support of a requisitioning authority command’s Procure-to-Pay (P2P) business process. E-commerce system user access management is one component of supply material management.

c. The scope of this Order is focused on those systems used for requesting, ordering, and performing receipt and acceptance of materials or services purchased by commands citing Marine Corps appropriations for both federal and commercial sources of supply; see enclosure (2) for a list of systems commonly used by the Marine Corps within P2P business process. Though the focus of this Order is on systems expending Marine Corps appropriations specifically within a P2P business process, it may be applied to any system as a template for implementing internal controls to meet the commander’s control objectives, as defined in reference (a).

d. Efficient and effective use of E-commerce systems requires the implementation of access controls, an engaged hierarchy of logistics management oversight, and system advocacy from headquarters. This Order codifies necessary roles and responsibilities of unit-level Commanding Officers/Accountable Officers (COs/AOs), higher echelons of the chain of

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

command, and Headquarters Marine Corps (HQMC).

e. This is a new Order and shall be read in its entirety. This Order is in accordance with references (a) through (q).

2. Mission. Establish clear roles, responsibilities, and procedures to ensure effective E-commerce system access management and internal controls.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Establish Marine Corps policy for access management and internal controls over E-commerce systems used by the Marine Corps. This will strengthen end-to-end requisition management, to include those actions that result in or from procurement activities, while meeting the standards and requirements established in references (a) through (q).

(2) Concept of Operations. This Order codifies requirements for user access controls at the requisition authority level and management oversight of E-commerce system usage by the supporting logistics hierarchy.

b. Subordinate Element Missions

(1) Deputy Commandant for Installations and Logistics (DC I&L)

(a) Appoint in writing HQMC system advocates for each E-commerce system used within the P2P business process.

(b) On a semi-annual basis in the 2nd and 4th quarter, publish E-commerce system user access listings via tasker to facilitate the semi-annual user account review and certification of E-commerce systems.

1. The tasker will require the submission of an inventory of E-commerce systems used throughout the commands, with the primary User Access Managers (UAMs) identified per Department of Defense Activity Address Code (DoDAAC), as an enclosure to the major command certification.

2. The tasker will require the submission of appointment and access authority documentation for a random sample of users within the E-commerce systems for each major command, as an enclosure to the major command's certification.

(c) Review proposed E-commerce system change requests (SCRs) for accuracy, validity, and recommended order of priority and potential funding. Major command SCRs must be evaluated to determine whether the request is due to a lack of training or a true gap in system capability that inhibits efficiency or impedes compliance with policy, prior to forwarding to the Functional Review Board (FRB) or system advocate.

(d) Evaluate compliance with this Order via the Internal Controls and Audit Readiness Team (ICART) and regional Field Supply and Maintenance Analysis Office (FSMAO) inspections.

(e) Coordinate compliance with this Order and semi-annual user access review certification with the command's Risk Management and Internal Control (RMIC) Program coordinator for submission as part of the annual statement of assurance (SOA) over P2P E-commerce system user access controls.

(2) Major Command. Command immediately subordinate to HQMC (e.g., Marine Forces Commands (MARFORs), Training and Education Command (TECOM), Marine Corps Systems Command (MCSC), Marine Corps Installations Command (MCICOM), Marine Corps Recruiting Command (MCRC), etc.).

(a) Coordinate and consolidate the user access review certifications and enclosures submitted by parent commands to the major command. The major command will submit one certification for the major command, with enclosures from all parent/subordinate commands consolidated, to HQMC Installations and Logistics, as part of the semi-annual tasker.

(b) Via DD Form 577, "Appointment/Termination Record - Authorized Signature," appoint a major command UAM for the Procurement Integrated Enterprise Environment (PIEE) Wide Area Workflow (WAWF) application, which is the Government Administrator (GAM) role, for the major command's DoDAAC. Authority to sign the PIEE GAM DD Form 577 for the non-requisition authority command will reside with the Assistant Chief of Staff or Director of the staff section which the GAM appointee is aligned by the table of organization. The PIEE application user administration capability provides a hierarchy that supports provisioning of parent/subordinate command GAMs. The PIEE WAWF GAM is specifically to support the P2P business process. The major command PIEE GAM will comply with UAM responsibilities contained in this Order.

(c) Coordinate compliance with this Order and semi-annual user access review certification with the major command's RMIC Program coordinator for submission as part of the command's annual SOA over P2P E-commerce system user access controls.

(d) Review proposed E-commerce SCRs for accuracy, validity, and recommended order of priority and submit to Deputy Commandant for Installations and Logistics (DC I&L). Parent command SCRs must be evaluated to determine whether the request is due to a lack of training or a true gap in system capability that inhibits efficiency or impedes compliance with policy, prior to forwarding up the chain of command.

(3) Parent Command. Examples of parent commands are Major Subordinate Command (MSC), Marine Corps Base (MCB), Marine Corps Air Stations (MCAS), Recruiting Districts, etc. While most parent command DoDAACs are authority code 02, some parent command DoDAACs are authority code 05 (e.g., the Marine Expeditionary Force (MEF) is the parent command for the Marine Expeditionary Units (MEUs) and the MARFORs are a parent command to their headquarters battalion or other stand-alone battalions immediately subordinate). Responsibilities include the following:

(a) Ensure subordinate command primary UAMs are identified, formally appointed, and trained on the requirements of this Order; the user administration functionality within the system is assigned; and the P2P business process for each E-commerce system is used; for each organization within the parent command's span of control.

(b) Appoint via DD Form 577 a parent command UAM for the PIEE WAWF application, which is the GAM role, for the parent command's DoDAAC. Authority to sign the PIEE GAM DD Form 577 for the non-requisition authority command will reside with the Assistant Chief of Staff or Director of the staff section which the GAM appointee is aligned by the table of organization. The PIEE application user administration capability provides a hierarchy that supports provisioning of subordinate command GAMs. The PIEE WAWF GAM is specifically to support the P2P business process. The parent command PIEE GAM will comply with UAM responsibilities contained in this Order.

(c) Ensure P2P business process system training is available and web links to material or physical training material is provided to subordinate commands as needed.

(d) Ensure the availability of an on-site/local area helpdesk/ subject matter expert (SME) support capability for any E-commerce system used by subordinate commands in the performance of a P2P business process.

(e) Ensure a semi-annual review and certification of E-commerce system user accounts is conducted by the subordinate commands and that the certification complies with requirements listed in this Order for user access provisioning.

1. Semi-annual review certifications submitted by subordinate commands to the parent command must be consolidated by the parent command. The parent command will submit a certification of completion of review and compliance with requirements of this Order, using enclosure (3), to the next senior command.

2. During the review, an inventory must be taken of all E-commerce systems, within a P2P process, to ensure all systems are accounted for with a primary UAM assigned. The system inventory and primary UAM assigned will be reported to the next senior command as an enclosure to the parent command's certification.

(f) Monitor and enforce timely resolution of P2P business process errors received from internal or higher headquarters generated reports/taskers (i.e., unprocessed receiving reports, invoices identified as delinquent, missing obligations/prevalidation failures, unmatched disbursements, etc.).

(g) Coordinate compliance with this Order and semi-annual user access review certification with the command's RMIC Program coordinator for submission as part of the command's annual SOA over P2P E-commerce system user access controls.

(h) Review proposed E-commerce SCRs for accuracy, validity, and recommended order of priority and submit them to the next senior command. Subordinate command SCRs must be evaluated to determine whether the request is due to a lack of training or a true gap in system capability that inhibits efficiency or impedes compliance with policy, prior to forwarding up the chain of command.

(4) Commanding Officer / Accountable Officer (CO/AO)

(a) Primary responsibility for the provisioning of system access and the maintenance of that access belongs to the CO/AO of the DoDAAC for which the access is provisioned. This responsibility is delegated by the CO/AO to the appointed UAM.

(b) Maintain a documented inventory of all E-commerce systems used by the command within a P2P business process.

(c) Appoint a primary UAM for each E-commerce system used by the command within a P2P business process, per volume 1 of reference (j).

1. Per volume 1 of reference (j), the role of Automated Information System (AIS) administrator, also called UAM, is inherent to the supply officer/Accountable Property Officer (APO) billet and must be identified in the appointment of the supply officer/supply resource manager by the CO/AO. To further delineate the requirement, the system(s) which the supply officer is appointed the UAM must be specifically called out in the appointment for any system utilized by the command in a P2P business process. See enclosure (2) for a list of commonly used P2P systems.

2. Users provisioned as a UAM for the CO/AO should be selected based on their knowledge and experience with the E-commerce system appointed to administer and/or with the individual's responsibility for management/oversight of the system access being appointed to administer; for this reason, the rank/grade of appointed UAMs should be commensurate, (e.g., Staff Non-Commissioned Officers (SNCOs), warrant or commissioned officers, or civilian-equivalent grades); contract personnel may also be appointed as needed.

3. For systems that provide an internal user administration capability, in the event more than one individual is provisioned with UAM access, the UAM appointments must delineate primary from alternate UAMs for the command.

(d) Ensure a semi-annual review and validation of E-commerce system users for the command is conducted. Reviews must verify compliance with this Order. Completion of the review must be certified using enclosure (3) and include the command's inventory of E-commerce systems used within a P2P business process and the primary UAM appointed per system.

(5) User Access Manager (UAM) Responsibilities. UAMs are responsible for performing or coordinating user activation/deactivation and assignment of roles/permissions in E-commerce systems at the unit level and maintenance of all pertaining requirements. Specific UAM responsibilities include the following:

(a) Ensuring a check-in/check-out procedure is implemented and working effectively for new or departing members of the command that specifically includes the applicable UAM for any provisioned P2P system access.

(b) Provisioning System Access

1. Prior to the activation of any user's requested system access, review the user's DD Form 2875, "System Authorization Access Request (SAAR)," to ensure all applicable boxes are filled in, with specific emphasis on the following:

a. Signed and dated by the user.

b. Signed and dated by the user's current supervisor.

c. Information assurance training certification date is current and certificates are provided with the SAAR, which includes Personally Identifiable Information (PII) and Cyber Security Awareness Training Certificates.

d. System access or role requested is supported by valid and verifiable justification.

e. Any specific data attribute requirements of the DD Form 2875 by the information assurance officer (IAO) or information owner (IO) are adhered to.

f. Signed and dated with security information by the security manager, if applicable.

g. Signed and dated by the IAO and/or IO, if applicable.

2. Ensure that, if the system access or role being activated is in the capacity of a final authorizing official, for the approval of a purchase request, the user’s SAAR is supported with a DD Form 577 and appointment letter per volume 3 of reference (j) and with current financial approver certificates of completed training as identified in reference (l).

3. Ensure that, if the system access or role being activated is limited to requesting materials or services, that the user’s SAAR is supported with either a NAVMC 11869, “Notice of Delegation of Authority” (DOA) Form, or by a responsible officer appointment letter, per volume 3 of reference (j).

4. Ensure that, if the system access or role being activated is in the capacity of a departmental accountable official (DAO), per volume 5, chapter 5 of reference (e), or as an invoice certifying officer, the user’s SAAR is supported by a DD Form 577 and appointment letter per volume 3 of reference (j). Per this order, the WAWF Acceptor role is considered a DAO and must be appointed via the DD Form 577.

5. Ensure DAOs and certifying officers have completed a Department of Defense (DoD) Certifying Officer Legislation (COL) Training Course and the current certificate is provided with the SAAR, per reference (e). Per this order, the COL training requirement is being levied upon DAOs within the P2P business process, specifically, the WAWF Acceptor role.

6. Prior to activating the user’s requested access, ensure that the request does not constitute a segregation of duties (SOD) conflict with other provisioned system access for the user or any manual roles performed by the user. SOD considerations are outlined in volume 5 of reference (j).

7. Ensure view-only roles within an E-commerce system, or system reporting functionality, are limited to the SAAR, unless otherwise specified by the system owner.

8. All provisioning documentation and training certificates must be uploaded into the system in which the access is provisioned if the system supports uploading of attachments. For systems that do not provide the ability to upload documentation, the UAM will maintain the documentation physically or electronically in accordance with supply records retention

requirements in volume 3 of reference (j).

9. For any system that provides the capability to limit the user’s provisioned access to a date range (e.g., end date the access at a specific point in time), the user’s end of active service (EAS) date or anticipated rotation date (permanent change of station (PCS) or end of temporary duty) from the command should be used.

10. For departing members of the command, prior to endorsing the user's check-out sheet, UAMs must remove the user’s E-commerce system access or roles associated to the command. SAAR Forms must be retained in accordance with supply records retention requirements identified in volume 3 of reference (j) following termination of a user's access to the command DoDAAC or system.

11. For systems that do not provide a user administration capability, removal of a user’s system access must be requested via the system owner. Positive confirmation of removal of the user’s access by the system owner must be retained by the UAM in accordance with supply records retention requirements identified in volume 3 of reference (j) to support termination of the user’s access to the system.

(c) As part of the supply officer internal controls review program, reference (m), and semi-annual tasker; perform; and document an E-commerce system access review during the 2nd and 4th quarter of each fiscal year. The review must verify compliance with all user access management requirements identified in this order.

1. During the review, any active system user missing required appointment documentation or training certificates required to support the approved access, or if an SOD conflict is identified, the user’s access must be suspended until the issues are resolved or system access must be removed completely if unable to resolve.

2. Completion of user access reviews must be certified using the format contained in enclosure (3) and maintained per supply records retention requirements in volume 3 of reference (j).

3. During the review, an inventory must be taken of all E-commerce systems used within a P2P business process, to ensure all systems are accounted for with a primary UAM assigned. The system inventory and primary UAM assigned will be reported to the parent command as an enclosure to the certification.

(d) Reset user account passwords or certificates as needed.

(e) Provide system users with training materials or links to available training as needed, for the use of the systems/roles used within the P2P business process.

(f) Gain and maintain SME functional knowledge regarding the overall use of and roles within the system and P2P business process, to provide a SME UAM capability to the command and help desk support to all system users within.

(g) Submit E-commerce SCRs determined to be necessary by the command to the parent command.

4. Administration and Logistics

a. Records Management. Records created as a result of this Order shall be managed according to National Archives and Records Administration (NARA)-approved dispositions in reference (n), SECNAV M-5210.1, to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium. Records disposition schedules are located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to reference (o), MCO 5210.11F, for Marine Corps records management policy and procedures.

b. Privacy Act. Any misuse or unauthorized disclosure of 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 reference (p), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended, and implemented in reference (h), SECNAVINST 5211.5F.

c. Forms. Forms used in this Order are: DD Form 577, DD Form 2875, and NAVMC 11869.

d. Updates. Updates made to this Order shall be done in accordance with the current iteration of reference (q), MCO 5215.1, “Marine Corps Directives Management Program.”

e. Recommendations. Recommendations concerning the contents of this Order are welcomed and may be forwarded to the DC I&L (Attn LP) via the appropriate chain of command.

5. Command and Signal

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

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

E. D. BANTA
Deputy Commandant for
Installations and Logistics

DISTRIBUTION: PCN 10255306000

References

(a) Memorandum to the Heads of Executive Departments and Agencies, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016
(b) "Federal Information System Controls Audit Manual (FISCAM)," February 2, 2009
(c) NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020
(d) NIST Special Publication 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," May 2010
(e) DoD 7000.14-R, "Financial Management Regulation," December 2021
(f) DoDD 8190.01E w/CH-3, "Defense Logistics Management Standards (DLMS)," December 30, 2019
(g) Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, "Financial Improvement and Audit Readiness (FIAR) Guidance," April 3, 2017
(h) SECNAVINST 5211.5F
(i) Marine Corps Manual w/CH-3, Chapter 4
(j) MCO 4400.201 w/CH-2
(k) MCO 5200.24E
(l) MARADMIN 350-11
(m) NAVMC 4000.5D
(n) SECNAV M-5210.1
(o) MCO 5210.11F
(p) 5 U.S.C. § 552a
(q) MCO 5215.1K w/Admin CH-1

Commonly Used Systems

System	Description
Defense Agency's Initiative (DAI) I-Procurement	I-Procurement is the Marine Corps purchase order request system for placing requests for contractual procurement, along with other types of purchases.
Defense Logistics Agency (DLA) Data Services Online	Formerly Navy Forms Online, this website is used for ordering forms and printing services.
Defense Logistics Agency (DLA) Enterprise External Business Portal (EEBP)	The DLA EEBP provides both reporting capabilities to track the ordering and over-the-counter purchasing of fuels and a fuel ordering platform used primarily by installation commands.
Defense Logistics Agency (DLA) Federal Mall (FEDMALL)	DLA FEDMALL provides access to requisitions, research, and tracking tools for DLA inventory.
Defense Automatic Addressing System (DAAS) Web Portal – Web Requisitioning (WEBREQ)	WEBREQ provides customers a means to input requisitions, cancellations, follow-ups, modifications, and Materiel Obligation Validation (MOV) documents.
Defense Medical Logistics Standard Support (DMLSS)	DMLSS is used by the Medical Logistics (MEDLOG) Battalion within the Marine Logistics Groups (MLGs) to purchase medical and dental supplies (Class VIII).
Fleet Commander Online (U.S. Bank)	Commercial fuel card program vendor application used to certify and pay non-fuel purchases and management of cards.
Global Combat Support System - Marine Corps (GCSS-MC)	Primary MILSTRIP requisitioning platform for the Marine Corps.
General Services Administration (GSA) USMC ServMart, Global Supply, Advantage	From office supplies and tools to furniture or cleaning products, GSA's web platforms offer requisitioning for hundreds of thousands of products.
Marine Corps Food Management Information System (MCFMIS)	Marine Corps system used to request subsistence.
Navy Supply Systems Command (NAVSUP) One Touch Support (OTS)	The NAVSUP OTS program capabilities include technical research, finding parts, requisitioning, and getting status.
Procurement Integrated Enterprise Environment (PIEE) Wide Area Workflow (WAWF)	WAWF allows commercial vendors to submit and track invoices and receipt/acceptance documents over the web. It also allows government personnel to process those transactions in a real-time environment.
Subsistence Total Order and Receipt Electronic System (STORES)	DLA prime vendor system used to purchase subsistence via MILSTRIP.
SAIC PURCHASE PLACE	A DLA prime vendor web portal for placing MILSTRIP or MIPR orders.
Transportation Capacity Planning Tool (TCPT)	TCPT, a "bridge technology," is used to provide near-term transportation planning, management, and execution capabilities to the operating forces.
USMC MAXIMO (USMCmax)	USMCmax is the MCICOM-sole computerized maintenance management system (CMMS) used by facilities maintenance activities.

Certification Template

UNIT LETTER HEAD

4XXX
Section
DD MMM YYY

From: Assistant Chief of Staff G-4, *(Enter Command)*
To: Assistant Deputy Commandant, Installation and Logistics (LP)

Subj: ### QUARTER USER ACCESS REVIEW CERTIFICATION

Ref: (a) Marine Corps Order 4###
(b) ETMS2 Tasker – DON-XXXXXX-XXXX

Encl: (1) E-commerce system inventory and primary UAM assigned per DoDAAC
(2) Users to remove from GSA (or other) systems (if applicable)

1. Per reference (a), a semi-annual user access review and validation has been conducted based on access listings provided in reference (b) for all users aligned to Department of Defense Address Activity Codes (DoDAACs) under this command. The review performed ensured the following:

a. Current and applicable training certificates exist for all roles assigned. The current DD 2875s exist signed by appropriate authority and are specific to the system(s) and role(s) assigned to the user.

b. Current appointment documentation and DD Form 577s exist and are signed by appropriate authority for users with a funds approver/certifier, requisition or purchase request approver, or invoice acceptor/certifier role.

c. Current appointment documentation exists and is signed by appropriate authority. This includes assigned user access managers (UAMs) for each system used by each entity/DoDAAC performing requisitioning, purchasing, or processing purchase requests for payment/invoices (see enclosure (2)).

d. Segregation of duties (SOD) considerations have been reviewed for each user’s system access and role assignment, within the business process, and no SOD violations has been identified.

e. Users no longer requiring access to systems have been removed, except for those identified in enclosure (3).

2. Please contact (*enter action officer point of contact name/email/phone*) if you have any questions.

O6/GS-15 Authorized

APPENDIX A

Glossary of Acronyms and Abbreviations

AIS	Automated Information System
AO	Accountable Officer
APO	Accountable Property Officer
CMMS	Computerized Maintenance Management System
CO	Commanding Officer
COL	Certifying Officer Legislation
DAAS	Defense Automatic Addressing System
DAI	Defense Agency's Initiative
DAO	Departmental Accountable Official
DC I&L	Deputy Commandant for Installations and Logistics
DLA	Defense Logistics Agency
DMLSS	Defense Medical Logistics Standard Support
DOA	Delegation of Authority
DoD	Department of Defense
DoDAAC	Department of Defense Activity Address Code
DON	Department of the Navy
DON/AA	Department of the Navy/Assistant for Administration
DRMD	Directives and Records Management Division
EAS	End of Active Service
E-commerce	Electronic Commerce
EDI	Electronic Data Interchange
EEBP	Enterprise External Business Portal
FEDMALL	Federal Mall
FIAR	Financial Improvement and Audit Readiness
FISCAM	Federal Information System Controls Audit Manual
FRB	Functional Review Board
FSMAO	Field Supply and Maintenance Analysis Office
GAM	Government Administrator
GCSS-MC	Global Combat Support System - Marine Corps
GSA	General Services Administration
HQMC	Headquarters Marine Corps
IAO	Information Assurance Officer
ICART	Internal Controls and Audit Readiness Team
IO	Information Owner
I&L	Installations and Logistics
MARFOR	Marine Forces Command
MCAS	Marine Corps Air Stations
MCB	Marine Corps Base
MCFMIS	Marine Corps Food Management Information System
MCICOM	Marine Corps Installations Command
MCRC	Marine Corps Recruiting Command
MCSC	Marine Corps Systems Command
MEDLOG	Medical Logistics
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MLG	Marine Logistics Group

MOV	Materiel Obligation Validation
MSC	Major Subordinate Command
NARA	National Archives and Records Administration
NAVSUP	Navy Supply Systems Command
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTS	One Touch Support
P2P	Procure-to-Pay
PCS	Permanent Change of Station
PIEE	Procurement Integrated Enterprise Environment
PII	Personally Identifiable Information
RMIC	Risk Management and Internal Control
SAAR	System Authorization Access Request
SCR	System Change Request
SME	Subject Matter Expert
SNCO	Staff Non-Commissioned Officer
SOA	Statement of Assurance
SOD	Segregation of Duties
STORES	Subsistence Total Order and Receipt Electronic System
TCPT	Transportation Capacity Planning Tool
TECOM	Training and Education Command
UAM	User Access Manager
UMX	User Management
USMCmax	USMC MAXIMO
UUAM	Unit User Account Manager
WAWF	Wide Area Workflow
WEBREQ	Web Requisitioning

APPENDIX B

Glossary of Terms and Definitions

1. Access Management. Controls implemented to limit system access to only authorized individuals and only for those specific purposes the individuals are authorized to perform.

2. Electronic Commerce (E-commerce). 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.

3. Major Command. Command immediately subordinate to HQMC (e.g., MARFORs, TECOM, MCSC, MCICOM, MCRC, etc.).

4. Parent Command. For the purposes of this Order, the first non-requisition authority command in the chain of a requisition authority command is considered the parent command (e.g., MSC, MCB, MCAS, Recruiting Districts, etc.). While most parent command DoDAACs are authority code 02, some parent command DoDAACs are authority code 05 (e.g., the MEF is the parent command for the MEUs and the MARFORs are a parent command to their headquarters battalion or other stand-alone battalions immediately subordinate).

5. Procure-to-pay (P2P). Per reference (g), P2P encompasses the business functions necessary to obtain goods and services. This includes functions such as requirements identification, sourcing, contract management, purchasing, payment management, and receipt and debt management. DC I&L (I&L) is the business Process Owner for the P2P process.

6. Provisioning. The process a UAM follows to activate or deactivate a user’s access to a system or specific functionality within a system.

7. User Access Manager (UAM). Per volume 1 of reference (j), the supply officer is inherently the AIS administrator for the requisition authority command and is responsible for maintaining access controls to systems which expend the command’s appropriated dollars. E-commerce systems that provide an internal user administration capability have various descriptions for the system role that is used to perform those functions (e.g., Unit User Account Manager (UUAM), GAM, User Management (UMX), etc.). There are also E-commerce systems that do not provide an internal user administration capability. For the purpose of this Order, the individual appointed the responsibility for system access management, regardless of the system, will be referred to as the UAM.